Greatham Church of England Online Safety Policy

Background/Rationale

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 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 at Greatham Church of England Primary School are bound.

The Greatham Online Safety Policy should help to ensure safe and appropriate use. The development and implementation of our strategy has involved all the stakeholders from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the 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 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 (nudes/semi nudes) 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 the Greatham Online Safety Policy is used in conjunction with other school policies (e.g. our Behaviour and Bullying Policy and all Safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build 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.

We must demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The Greatham Online Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

This Online Safety policy has been developed by our Online Safety Committee made up of:

• the Headteacher;

• the Deputy Headteacher;

• the Online Safety Coordinator;

• the Online Safety Link Governor;

• the SENCo;

• members of the School Council;

• a teacher representative;

• a teaching assistant representative;

• a parent representative;

• the school's ICT Technician.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, 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 of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Greatham Online Safety Policy and for reviewing the effectiveness of the policy and holding the headteacher to account for its implementation.

. This will be carried out by the Pupil and Personnel Subcommittee receiving regular information about Online Safety incidents and monitoring reports.

A member of the Governing Body has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

• regular meetings with the Online Safety Coordinator;

• regular monitoring of Online Safety incident logs;

• regular monitoring of Local Authority Policy Central Monitoring Software reports;

• reporting to relevant Governors committee/meeting.

Headteacher:

• the Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Coordinator;

• the Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant;

• the Headteacher ensures that there is a system in place to allow for monitoring and

support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. For example, there is additional support provided through Space To Learn, the South Hartlepool Family of Schools, the LA ICT Network and the school's ICT Technician;

• the Headteacher receives regular monitoring reports from the Online Safety Coordinator;

• the Headteacher and Deputy Headteacher (in the Headteacher's absence) are aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Online Safety Coordinator:

• leads the Online Safety committee;

• ensures that he/she keeps up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant;

• takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the Greatham Online Safety Policy;

• ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;

• ensures that monitoring software/systems are implemented and updated as agreed in school policies;

• provides training and advice for staff;

• ensures that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed;

• ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place;

• ensures that the use of the network and school email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation/action/sanction;

• liaises with the Local Authority;

• liaises with school ICT technical staff;

• receives reports of Online Safety incidents and creates a log of incidents to inform future Online developments;

• meets regularly with the Online Safety Governor to discuss current issues, review incident logs and Local Authority Policy Central Monitoring Software reports;

• reports regularly to the Senior Leadership Team and Governing Body.

All staff and volunteers are responsible for ensuring that:

• They have an up to date awareness of Online Safety matters and of the current school online policy and practices;

• They have read, understood and signed the Acceptable Use Policy for Greatham Staff and Other Adults;

• They report any suspected misuse or problem to the Online Safety Coordinator for

investigation/action/sanction;

• Digital communications with pupils should be on a professional level and only carried out using official school systems;

• Online Safety issues are embedded in all aspects of the curriculum and other school activities;

• Pupils understand (as appropriate to their age) and follow the school Online Safety Policy and Acceptable Use Policy for Pupils;

• Pupils, as appropriate to their age, 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 Online Safety 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, 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.

The **designated person for child protection** should be trained in Online Safety 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 on-line contact with adults/strangers;

• potential or actual incidents of grooming;

• cyber-bullying.

Pupils

• are responsible for using the school ICT systems in accordance with the Online Safety Policy and from Year 3 onwards, pupils will sign the Acceptable Use Policy for Pupils before being given access to the school system;

• as appropriate to their age, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

• as appropriate to their age, need to understand the importance of reporting abuse,

misuse or access to inappropriate materials and know how to do so;

• as appropriate to their age, will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices;

• as appropriate to their age, know and understand school policies on the taking/use of images and on cyber-bullying;

• should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through the Online Safety section of the school website (as requested by parents/carers in the Parent/Carer Questionnaire).

Parents and carers will be responsible for signing the Acceptable Use Policy for Parents and Carers.

Other adults:

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Policy Statements

Education – pupils

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

Online Safety education will be provided in the following ways:

• A planned Online Safety programme is provided as part of ICT lessons at the start of every academic year and is regularly revisited – covering both the use of ICT and new technologies in school and outside school.

• Key Online Safety messages are reinforced as part of a planned programme of assemblies.

• Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

• Pupils are helped to understand the need for the Pupil AUP and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

• Pupils are 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 and the internet are displayed in all classrooms.

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

The school's Online Safety messages and rules are highlighted in the 'Online Safety' section of the school's website and information prominently displayed around school, particularly the school's 'SMART' rules.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

From September 2020, Relationships Education will be compulsory for all primary aged pupils, Relationships and Sex Education will be compulsory for all secondary aged pupils and Health Education will be compulsory in all state-funded schools in England.

Through these new subjects, pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.

This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example citizenship education covers media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

This advice supports schools to consider what they are already delivering through the curriculum, and build in additional teaching as required to ensure their pupils are receiving a fully rounded education with regard to online safety, both in terms of how to stay safe but also how to behave online.

Education – parents and carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line 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 raise parents’ awareness of internet safety in letters or other communications home, and in information via our website .

This policy will also be shared with parents.

Online safety will also be covered during parents’ evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training .

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the **acceptable use agreements**

Education & Training – Staff

We recognise that it is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal Online Safety training is available to staff. An audit of the online training needs of all staff is carried out regularly by the Online Safety Coordinator.

• All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies.

• The Online Safety Coordinator will receive regular updates through attendance at LA/other information/ training sessions.

• The Greatham Online Safety policy and its updates will be presented to and discussed by staff in staff briefings and meetings.

• The Online Safety Coordinator will provide advice/guidance/training to individuals as required.

Training – Governors

• Governors will take part in annual Online Safety training/awareness sessions, led by the Online Safety Coordinator and, where provided, by the Local Authority, National Governors' Association, and/or Hartlepool Governors' Association.

• Regular updates will also be provided by the Headteacher and/or Online Safety Coordinator as required/relevant.

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.

It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

• School ICT systems will be managed in ways that ensure that the school meets online technical requirements.

• There are regular reviews and audits of the safety and security of school ICT systems.

• Servers, wireless systems and cabling are securely located and physical access restricted.

• All adult users have clearly defined access rights to school ICT systems.

• All pupils (Year 1 to Year 6) are provided with an individual username and password and Reception pupils use a standard login.

• The "administrator" passwords for the school ICT system, used by the Network Manager and ICT Technician are available to the Headteacher and Online Safety Coordinator and are kept in a secure place.

• Users are 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 Local Authority Policy Central Monitoring

Software.

• In the event of the Network Manager (or other person) needing to switch off the

filtering for any reason, or for any user, this must be logged and carried out by the

Local Authority, as agreed by the Headteacher.

• Any filtering issues should be reported immediately to the Online Safety Coordinator.

• Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety Coordinator and Headteacher.

• The Local Authority regularly monitors and records the activity of users on the school ICT systems.

• An appropriate system is in place for users to report any actual/potential Online Safety incident to the Online Safety Coordinator. This is through verbally passing on details to the Online Safety Coordinator who records these and then takes appropriate action.

• Appropriate security measures are in place (via secure passwords) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

• An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system. Details are provided by the Headteacher of Online Safety Coordinator.

• Staff members are aware that no personal use is permitted on school laptops and other portable devices that may be used out of school.

• An agreed policy is in place that forbids staff from installing programs on school workstations/portable devices. Only the Network Manager, ICT Technician and Online Safety Coordinator are allowed to install programs.

• An agreed policy is in place regarding the use of removable media (e.g. memory

sticks/CDs/DVDs) by users on school workstations/portable devices. See the school’s AUP.

• The school infrastructure and individual workstations are protected by up to date virus software.

• Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum:

• In lessons where internet use is pre-planned, it is best practice that 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 pupils 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.

• It is accepted that, from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

• Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

• 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 pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and 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 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 members 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.

• All photographs should be stored on the school network which is password protected.

• Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the

school into disrepute (for example, photographs are never taken of children during swimming lessons).

• When pupils are given permission to take photographs (e.g. at sports events), they must follow the same rules as staff members and pass the camera (and memory card) back to the relevant member of staff immediately after the event.

• Pupils are allowed to take disposable cameras on educational visits, but not digital cameras, but pupils must not take, use, share, publish or distribute images of others without their permission.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the school's policy.

• Pupils' full names will not be used anywhere on the school website or in publication such as the school newsletter and the 'Hartlepool Mail', particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

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; and 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.

• The device must be password protected.

• The device must offer approved virus and malware checking software.

• The data must be securely deleted from the device, once it has been transferred or its use is complete.

Communications

Staff members are allowed to:

• bring mobile phones into school;

• use mobile phones in social time or in an emergency;

• use personal email addresses in school or on the school network in their own time, but not to send or receive work-related emails.

Pupils are not allowed to:

• bring mobile phones into school or on educational visits (including residentials) – if a mobile phone is found in school that is the property of a pupil, it will be removed, stored in

the Headteacher's or Deputy Headteacher's office and returned to the pupil at the end of the school day;

• use personal email addresses in school or on the school network.

Neither staff members nor pupils are allowed to:

• use mobile phones in lessons;

• take photos on mobile phones or any camera device other than a school camera;

• use chat rooms/facilities, instant messaging, social networking sites or any other kind of internet-based communication;

• use auction sites, gaming sites or gambling sites.

If a member of staff is unsure as to whether a website is appropriate or not, they should speak to the Headteacher.

When using communication technologies, the school considers the following as good practice:

• The official school email service is regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school or when sending and receiving work-related emails.

• Users need to be aware that email communications may be monitored.

• Users must immediately report to the Online Safety Coordinator 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 pupils or parents/carers (e.g. email, chat) 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 programs must not be used for these communications.

• 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 to identify members of staff.

Unsuitable/inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and is obviously banned from school and all other ICT systems. Other activities, e.g. Cyber-bullying, is and could lead to criminal prosecution. There are, however, a range of activities which may be legal, but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

• Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images;
- promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation;
- adult material that potentially breaches the Obscene Publications Act in the UK;
- criminally racist material in UK;
- pornography;
- promotion of any kind of discrimination;
- promotion of racial or religious hatred;
- threatening behaviour, including promotion of physical violence or mental harm;
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Using school systems to run a private business.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gaming (non educational).
- On-line gambling.
- On-line shopping/commerce.
- Use of social networking and dating sites.

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. In such cases, the following procedures should be followed:

• If a pupil or member of staff accidentally accesses inappropriate or illegal material, the

ICT device should be disconnected from the network and mains immediately, but should not be shut down. The teacher in charge of the class should then inform the Headteacher. The Headteacher will then contact the Local Authority and the police if the material is illegal.

• If a pupil suspects that someone is deliberately accessing inappropriate or illegal material, he/she should speak to his/her class teacher (unless it is the class teacher that the pupil suspects) or any other adult that he/she trusts. This adult should then inform the Headteacher. The Headteacher will then contact the Local Authority and the police if the material is illegal.

• If a member of staff suspects that someone is deliberately accessing inappropriate or illegal material, he/she should inform the Headteacher (or Deputy Headteacher if the member of staff suspects the Headteacher). The Headteacher (Deputy Headteacher) will then contact the Local Authority and the police if the material is illegal.

Sanctions are as follows:

• In the case of a pupil deliberately accessing inappropriate materials, sanctions will be imposed by the Headteacher in line with the child's parent(s)/carer(s).

• In the case of a pupil deliberately accessing illegal materials, sanctions will be imposed by the Headteacher in line with the child's parent(s)/carer(s) and criminal procedures will be followed.

• In the case of a staff member deliberately accessing inappropriate materials, sanctions will be imposed in line with the Local Authority Disciplinary and Capability Policy.

• In the case of a staff member deliberately accessing illegal materials, criminal procedures will be followed.

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 as follows:

Pupils: refer to the Headteacher if any of the below occurs:

• Deliberately accessing or trying to access material that could be considered illegal.

• Unauthorised use of non-educational sites during lessons.

• Unauthorised use of mobile phone/digital camera/other handheld device.

• Unauthorised use of social networking/instant messaging/personal email.

• Unauthorised downloading or uploading of files.

• Allowing others to access the school network by sharing username and passwords.

• Attempting to access or accessing the school network, using another pupil's account.

• Attempting to access or accessing the school network, using the account of a member of staff.

• Corrupting or destroying the data of other users.

• Creating or propagating computer viruses or other harmful files.

• Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.

• Continued infringements of the above, following previous warnings or sanctions.

• Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.

• Using proxy sites or other means to subvert the school's filtering system.

• Accidentally accessing offensive or pornographic material and failing to report the incident.

• Deliberately accessing or trying to access offensive or pornographic material.

• Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.

Staff: refer to the Headteacher if any of the below occurs:

• Deliberately accessing or trying to access material that could be considered illegal.

• Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email.

• Unauthorised downloading or uploading of files.

• Allowing others to access the school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.

• Careless use of personal data e.g. holding or transferring data in an insecure manner.

• Deliberate actions to breach data protection or network security rules.

• Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.

• Creating or propagating computer viruses or other harmful files.

• Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.

• Using personal email/social networking/instant messaging/text messaging to carry out digital communications with students/pupils.

• Actions which could compromise the staff member's professional standing.

• Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.

• Using proxy sites or other means to subvert the school's filtering system.

• Accidentally accessing offensive or pornographic material and failing to report the incident.

• Deliberately accessing or trying to access offensive or pornographic material.

• Breaching copyright or licensing regulations.

• Continued infringements of the above, following previous warnings or sanctions.

For further information see: Teaching online safety in school and Acceptable Use Policy

Chair of Governors……Date