NUTGROVE METHODIST AIDED PRIMARY SCHOOL

E-SAFETY AND INTERNET POLICY
Reviewed February 2016

INTRODUCTION

At Nutgrove we believe that "Computing should not be taught in isolation, but is a tool that should be used and embedded in all subjects." (Computing Policy), therefore all pupils should have access to the internet and digital communication to enhance their learning across all subject areas.

The safety of our pupils at Nutgrove is of the utmost importance. Information communication technology is changing at an incredible pace and it is our shared responsibility to ensure our pupils have full access to technology whilst remaining safe and secure.

This document outlines the way in which we, as a school, protect and safeguard our pupils and parents from the potential dangers of using technology to communicate over the Internet.

This policy has been developed to allow any persons to make best use of the Internet whilst at the same time safeguarding everyone who uses it.

Purpose

The purpose of this policy is to specify the rules in relation to users of the Internet, both within our school and when using school equipment at home. The policy is provided to protect schools, governing bodies and the user from risks associated with Internet usage. This Policy applies to all members of staff and pupils within our school**.**

Rationale

When online, we believe that children and young people may be vulnerable and can expose themselves to danger, whether knowingly or unknowingly, when using the Internet and other technologies.

This document will serve as a guide for staff and reference for parents, governors and other adults (including volunteers).

What are the risks?

The Byron review has classified the risks as relating to content, contact and conduct. The risks are often determined by behaviors rather than technology themselves.

	Commercial	**Aggressive**	**Sexual**	**Values**
Content (child as a recipient)	Adverts Spam Sponsorship Personal info	Violent Hateful content	Pornographic or unwelcome sexual content	Bias Racial Misleading info or advice
Contact (child as a participant)	Tracking Harvesting Personal info	Being Bullied, Harassed or stalked	Meeting strangers Being Groomed	Self-Harm Unwelcome Persuasions
Conduct (child as an actor)	Illegal downloading Hacking Gambling Financial Scams	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info and advice

The 4 categories of risks outlined in top row of the above diagram form the basis for safeguarding our pupils. Indeed, our school internet filtering system uses these categories when deeming which sites are appropriate. The filtering section is described in more detail in the next section.

MONITORING OF INTERNET USAGE

All Staff/Parents/Governors should be aware that Internet access in school is logged by the filtering system (Symantec Web Security) and that logs indicating the number and types of web sites that have been accessed by members of staff are subject to review by Senior Education Manager's and Head Teachers.

Members of staff using school equipment to access the Internet at home should be aware that the Council's Audit team will, from time to time, make requests for computer equipment to be made available to them for analysis/investigation. Members of staff should be aware that this will not just occur when inappropriate use has been proved, or is suspected but on a random basis.

Members of staff should be aware that all Internet activity, using the 'sthelens.org.uk' e-mail accounts, are constantly monitored, through the MailGear software, for inappropriate language.

Use of other e-mail accounts will be monitored through random sampling as outlined in the paragraph above.

Any inappropriate access/attempts to access the internet or e-mail activity will be investigated and may lead to disciplinary action being taken against members of staff. Disciplinary action may take the form of Gross Misconduct/Misconduct depending on the severity of the breach of the policy. Any inappropriate access of a criminal nature will be reported to the Police, or any other relevant agencies that the Local Authority deems appropriate.

There should be no expectation of privacy in Internet or e-mail usage by individuals.

The school reserves the right to inspect any and all files stored in private areas of the network or on disc in order to assure compliance with this policy.

In line with council strategy all logs of Internet usage are kept for 6 months.

At Nutgrove we expect all staff using ICT Equipment to monitor the pupils Internet access as this will enable early notice of inappropriate use by individuals. In such cases this will be immediately reported to the Headteacher and the issue will be dealt with in line with our behaviour policy. If, in the course of their approved used, they come across any inappropriate material, Form 1 should be completed with appropriate details and sent to Agilysis to remove the access to the site immediately. (Form 1 can be found at the end of this policy).

We also require permission slips from parents and carers to agree for pupils to use the Internet within school. These are then kept in the pupils personal files in the school office.

Policy Statement for All Staff

The Governing Body recognises the internet is an important resource for teaching, learning, personal development and an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential of ICT and communications systems to enhance and develop all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that pupils are protected from contact with inappropriate material.

In addition to their normal access to the school's ICT and communications systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and e-mail and internet facilities during their own time subject to such use:

- not depriving pupils of the use of the equipment
- not interfering with the proper performance of the staff member's duties

Whilst the school's ICT systems may be used both for work and personal use as described above, the Governing Body expects use of this equipment to be appropriate, courteous and consistent with the expectations of the Governing Body at all times.

This policy covers the use of all school-owned equipment and communications, examples of which may include:

- Laptops and personal computers;
- ICT network facilities;
- iPads;
- Handheld computers;
- Mobile phones;
- USB keys and other online storage devices;
- Image data capture and storage devices including cameras and video equipment.

This list is not exhaustive

THE USE OF SCHOOL ICT AND COMMUNICATIONS FACILITIES/EQUIPMENT

Staff:

- Must be responsible;
- Must keep equipment safe;
- Must not share, and must always treat as confidential, any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries;
- Must report known breaches of this policy, including any appropriate images or other material which may be discovered on the school's ICT systems;
- Must report to the Head Teacher any vulnerabilities affecting child protection in the school's ICT and communications systems;
- Must not install software on the school's equipment, including freeware and shareware, unless authorised by the Agilysis team member;
- Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures;

- Must ensure that any equipment is used in compliance with this policy;
- Must store any personal information about pupils on an encrypted pen drive and not on laptops.

ANYONE USING THE INTERNET WITHIN OUR SCHOOL MUST NOT:

- Make, gain access to, publish or distribute inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read it;
- Make, gain access to, publish or distribute material promoting homophobia or racial or religious hatred;
- Use it for the purpose of bullying or harassment, or in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation;
- Use it for the publication and/or distribution of libelous statements or material which defames or degrades others;
- Use it for the publication and distribution of personal data without authorization;
- Use it for the publication of material that defames, denigrates or brings into disrepute the school and/or its staff and pupils;
- Email correspondence that is unlawful or in pursuance of unlawful activity, including unlawful discrimination;
- Participate in on-line gambling;
- Infringe copyright law;
- Gain unauthorised access to internal or external computer systems (hacking);
- Create or deliberately distribute ICT or communications "malware" including viruses, worms etc;
- Record or monitor telephone or e-mail communications without the express approval of the governing body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has established for that such action is in full compliance with all relevant legislation and regulations (see Regulation of Investigatory Powers Act 2000, below);
- Enable or assist others to breach the Governors' expectations as set out in this policy.

INTERNET ACCESS AT HOME USING SCHOOL EQUIPMENT

Some members of staff have access to school computer equipment (laptops and iPads) which they are able to use at home. It is recognised that when using such devices within their own home, staff will have greater freedom in relation to activities such as on-line shopping. When members of staff are using such equipment for personal use at home the following rules apply.

Members of staff should not use, or try to use, the Internet for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to School policy.

Where access to such sites occurs accidentally this should be reported to the Head Teacher as soon as possible.

Members of staff must be aware of, and abide by, the Data Protection Act as its provisions cover data transmitted and stored on e-mail.

Any downloaded software should be properly licensed and registered. The downloading of music or data must not breach the rights of copyright owners.

Users should not use, or try to use, the Internet to break through security controls (i.e. hacking).

Users should not do anything which is illegal under English law or the law of any other relevant country.

Users should not use, or try to use, the Internet to intentionally access or transmit computer viruses or similar software.

Only the member of staff to whom the computer has been loaned may use the computer to access the Internet. Allowing other family members or friends to use school equipment to access the Internet is strictly forbidden.

LOGGING ON

Foundation Stage, Key Stage 1 and Key Stage 2
All pupils in FS, KS1 and KS2 have a class user name and password. This allows them access to all software on the computer and a shared folder for their class. Within this folder each child has their own individual folder.

Staff, Students and Volunteers
All staff has their own individual user name and passwords. This allows full access to the school network e.g. access to all software on the computers and access to the staff share and pupil share folders. Staff is made aware that their folders can be accessed by any member of staff. Student teachers have their own log on details which gives them the same access as a child. They do not have access to the Staff Share folder. Volunteers are not to be given any log on details for the computers.

PUBLISHING ON THE WEB

Ground rules are important to ensure that the Web site reflects the school's ethos and that information is accurate and well presented. As the school's Web site can be accessed by anyone on the Internet, the security of staff and pupils must be considered carefully. Although common in newspaper reports, the publishing of pupils' names beside photographs that identify individuals may be considered inappropriate on Web pages.
While any risks might be small, the parents' perception of risk must also be taken into account in devising an appropriate policy.

- Editorial responsibility is delegated to a member of staff to ensure that content is accurate and quality of presentation is maintained;
- The Web site will comply with the school's guidelines for publications;
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name;
- The point of contact on the Website should be the school address and telephone number.
- Home information or individual e-mail identities will not be published;

- Photographs must not identify individual pupils. Group shots or pictures taken over the shoulder will be used in preference to individual "passport"' style images;
- Full names will not be used anywhere on the Website, particularly alongside photographs;
- Written permission from parents will besought before photographs of pupils are published on the school Website.

Conditions of Internet Use Policy

The school and Governing Body have agreed conditions for Internet Use. These rules and guidelines must be made available to all users in an appropriate format and kept under review. An 'Internet Use, Pupil Agreement' form is attached to this policy.

A copy of the agreement must be distributed to all users and pupils' parents/guardians and they must sign to acknowledge acceptance of the agreement. A copy of the 'Internet Use, Pupil Agreement' policy should be displayed in the ICT suite. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

This policy forms part of the school's ICT and Computing policy. Teachers, other staff, pupils and all other users are required to follow all the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access to the Internet and in some instances could lead to further appropriate action.

In the case of employees, any breach may also be considered a breach of the employee's conditions of service which could lead to appropriate disciplinary action including dismissal on grounds of gross misconduct.

Pupils are responsible for good behaviour on the Internet just as they are in a classroom or when representing the school in any way. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Parents/guardians permission is required. Access is seen as a privilege, not a right and that access to the Internet requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is agreed by all, that all users will comply with school guidelines and standards and will honor the agreements they have signed.

Any school storage areas, including those on Desktops, laptops, iPads, and any other storage device will be treated with respect and competently maintained at all times. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on any of the above storage systems would be private. Any documents pertinent to individual pupils will be stored on an encrypted storage system.

During school, teachers and staff will guide pupils towards appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, radio, newspapers, magazines, telephones, films and other potentially offensive material. Staff must also be careful

when setting homework, e.g. recommending particular sites to investigate or topics to research, etc.

Pupils will:

- Have equal access to email in a safe & secure environment;
- Have equal access to a variety of approved websites through the Internet;
- Pupils will be taught all the skills in order to use Internet & email as a computing tool;
- Pupils will use Internet & email to support, enhance & develop all aspects of their curriculum;
- Pupils will develop Internet & email skills at the appropriate level regardless of race, gender, intellect and emotional or physical difficulties.

NOTE

The above restrictions apply to the use of phones, e-mails, text messaging, internet chat rooms, blogs and personal websites (including entries onto myspace and facebook)

Regulation of Investigatory Powers Act 2000

Ancillary to their provision of ICT facilities, the Governing Body asserts the employer's rights to monitor and inspect the use by staff of any computer (including e-mails) or telephonic communications systems and will do so where there are grounds for suspecting that such facilities are being, or may have been, misused.

If you wish to report any violations of this policy you should inform the Headteacher or if necessary the St Helens Local Authority in line with the Whistle Blowing Policy. You will be dealt with in complete confidence

Any violations of the above policy will be thoroughly investigated and may result in disciplinary proceedings and if necessary, criminal proceedings.

POLICY AND GUIDANCE ON SCHOOL STAFF USE OF ICT AND COMMUNICATIONS SYSTEMS

PART 2: to be detached and placed on the employee's file

This declaration refers to the Governing Body's policy and guidance on the use of the school's ICT and communications systems and confirms that you have been provided with a copy and you have agreed to follow it.

All employees, supply staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

DECLARATION

You should sign two copies of this document: this copy will be retained in your personnel file.

I confirm that I have been provided with a copy of the school's E-Safety Policy and agree to the terms and conditions specified therein. I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies if I am working from home on school equipment or networks.

Signed:…….Date…….

Name:…….

Position in school:…….

NUTGROVE METHODIST AIDED PRIMARY SCHOOL INTERNET USE
Pupil Agreement

I will not access other people's files, or damage their work and data.

I will only use the Internet when I have permission and a teacher supervises me.

I will use the Internet only for activities and work set by school e.g. homework, class/topic work.

I will only Email people my teacher has approved, and not use the Internet for personal or private messages.

I will respect the privacy of others. I will not publish their names, addresses, phone numbers or photographs.

I will not give my home address or telephone number, or arrange to meet someone, through the Internet.

I will not use work from the Internet as if it was my own. I will give credit to the sources of materials included in my work.

I will not try to find or use inappropriate and unacceptable material from the Internet.

I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.

I will not use school resources to subscribe to any goods or services, nor buy or sell using the Internet.

I will not download software from the Internet unless this is authorised by the teacher.

I will not bring in removable storage drives, CD's or any electronic data from outside school unless I have been given permission.

I will not send unsuitable email messages. The messages I send will be polite, responsible and only signed in my name.

I will not send anonymous messages.

I will not take part in any activity that goes against school rules or government legislation.

I understand that the school may check my computer files and may monitor the Internet sites I visit.

Remember that access is a privilege, not a right and that access requires responsibility!

USE OF TECHNOLOGY OUTSIDE OF SCHOOL

As a school we are not responsible for the use of communication technology outside of school. This is a parental responsibility. We will follow the behaviour policy if any actions or comments from communication used out of school hours are brought back into school.

Please note: The legal age for a child to have a Facebook account is 13 years.

Leavers from the school

NOTIFICATION

REMOVAL OF INTERNET/E-MAIL ACCESS

Name _____

Post Held _____

Date Access is to Cease _____

I can confirm that I have notified Agilisys Service Desk of the above.

Authorised by Head Teacher _____

Date _____

FORM 1

NOTIFICATION

INADVERTENT ACCESS TO INAPPROPRIATE INTERNET SITES

Name _____

Post Held _____

Site Accessed _____

Date of Access _____

Time of Access _____

Reported by _____

I can confirm that I have notified Agilisys of the above.

Authorised by Head Teacher _____

Date _____