ST. ANNE'S CATHOLIC HIGH SCHOOL FOR GIRLS

Safeguarding: E-SAFETY POLICY

Contents

Mission Statement

St. Anne's Catholic High School for Girls will offer a positive presence in Enfield with a comprehensive curriculum delivered in modern facilities, equipping students with the ability to meet the challenges of the 21st Century confidently and with high spiritual and moral standards,

We recognise that students, parents, staff and governors make up the school's community which will continually self-evaluate to improve itself effectively and efficiently in all aspects of its growth.

We are a fully inclusive, Catholic girl's secondary school meeting high academic standards, promoting spirituality, pastoral care and the Catholic community.

We recognise in all our relationships the dignity and value of each person showing one another mutual acceptance and respect.

'Act justly, love tenderly, walk humbly with your God.'

1. Information on Internet Technology

It is commonly acknowledged that the educational and social benefits for children in using the internet should be promoted, but that this should be balanced against the need to safeguard children against the inherent risks from internet technology. At St. Anne's Catholic High School for Girls, we understand that we need to teach children to keep themselves safe whilst on-line.

This document summarises our e-safety strategy, designed to enable these aims to be achieved and support staff to recognise the risks and take action to help children use the internet safely and responsibly.

2. School E-Safety Strategies

2.1 Purpose and description

Computing is now a key part of the school curriculum and one of the key aims of computing is to ensure that pupils are aware of e-safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

The purpose of our e-safety strategy is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

In particular, we aim to ensure the following:

- A ***safe internet platform*** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (London Grid for Learning platform).
- A culture of ***safe practice*** underpinned by a strong framework of e-safety policy that ensures everyone is aware of expected standards of on-line behaviour.
- Children are ***taught to keep themselves and others safe*** on-line and use technology responsibly; we work in partnership with parents and carers to raise awareness of the potential risks of internet use.

2.2 Roles and responsibilities

2.2.1 Headteacher's role

- the overall development and implementation of the school's e-safety policy
- ensuring that e-safety issues are given a high profile within the school community
- linking with the board of governors and parents and carers to promote e-safety and forward the school's e-safety strategy
- ensuring e-safety is embedded in the curriculum
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies.

2.2.2 Governors' role

The governing body has a statutory responsibility for pupil safety and is aware of e-safety issues, providing support to the Headteacher in the development of the school's e-safety strategy.

Governors are subject to the same e-safety rules as staff members in order to keep them safe from allegations and ensure a high standard of professional conduct.

2.2.3 E-safety contact officer's role

The school's designated e-safety contact officer is Mrs Sanders, who is responsible for co-ordinating e-safety policies on behalf of the school. The e-safety contact officer is responsible for:

- developing, implementing, monitoring and reviewing the school's e-safety policy
- ensuring that staff and pupils are aware that any e-safety incident should be reported to them
- providing the first point of contact and advice for school staff, governors, pupils and parents
- liaising with the school's computing manager/co-ordinator to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the head teacher
- assessing the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- raising the profile of e-safety awareness with the school by ensuring access to training and relevant e-safety literature
- ensuring that all staff and pupils have read and signed the acceptable use policy (AUP)

2.2.4 Network manager's role

- the maintenance and monitoring of the school internet system including anti-virus and filtering systems
- carrying out monitoring and audits of networks and reporting breaches to the e-safety contact officer
- supporting any subsequent investigation into breaches and preserving any evidence.

2.2.5 Role of school staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- adhering to the school's e-safety and acceptable use policy and procedures
- communicating the school's e-safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the e-safety contact officer
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the e-safety contact officer

- teaching the e-safety and digital literacy elements of the new curriculum.

2.2.6 Designated child protection teachers

Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated child protection teacher for the school who will decide whether or not a referral should be made to Family Services and Social Work or the Police. The child protection officer is Mrs Gumbrell, Deputy Headteacher.

2.3 Working with parents and carers

Most of our children will have internet access at home or own mobile devices. Therefore, parents and carers need to know about the risks so that they are able to continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding. The school's runs e-safety training sessions for parents to support them and update their knowledge about developments in IT.

3. E-safety Policies

3.1 Accessing and monitoring the system

- Access to the school internet system is via individual log-ins and passwords for staff and pupils.
- The Network Manager keeps a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.
- Network and technical staff responsible for monitoring systems are line managed by Mrs Sanders, Deputy Headteacher.

3.2 Acceptable use policies

- All internet users within the school will be expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their internet use.
- Pupils and their parents should both sign the acceptable use agreement, and use of the internet in schools is dependent on signing this agreement (see Appendix 1).
- Staff are expected to sign an acceptable use agreement on appointment and this will be integrated into their general terms of employment (see Appendix 2).

The school office will keep a copy of all signed acceptable use agreements.

3.3 Teaching e-safety

One of the key features of the school's e-safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of e-safety education lies with the head teacher and the e-safety contact officer, but all staff should play a role in delivering e-safety messages.
- Teachers are primarily responsible for delivering an ongoing e-safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.
- Achievement Leaders may wish to use assemblies on e-safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.
- Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to.

3.4 IT and Safe Teaching Practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.
- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images on personal mobile devices erased.
- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.
- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.
- Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.
- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.
- Where staff need to communicate with pupils regarding school work, this should be via the school email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.
- When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.
- When making contact with parents or pupils by email, staff should always use their school email address or account. Personal email addresses should never be used.
- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.
- Where staff are using mobile equipment such as laptops or i-pads provided by the school, they should ensure that the equipment is kept safe and secure at all

times.

3.5 Safe use of technology

3.5.1 Internet and search engines

- Pupils are not allowed to aimlessly "surf" the internet and all use is expected to have a clearly defined educational purpose.
- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.
- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the e-safety contact officer, who will liaise with the IT service provider for temporary access. Teachers should notify the e-safety contact officer once access is no longer needed to ensure the site is blocked.

3.5.2 School website

- Content should not be uploaded onto the school website unless it has been authorised by the Headteacher who is responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.
- The school's designated person for uploading materials onto the website is Ms Geraci.
- To ensure the privacy and security of staff and pupils, the contact details on the website is the main school address, email and telephone number. No contact details for staff or pupils are given on the website.
- Children's full names are never be published on the website.
- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

3.5.3 Photographic and video images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images are carefully selected so that individual pupils cannot be easily identified. Group photographs are used where possible.
- Parents and cares sign an agreement to indicate their permission for their child's photo to be used on the website or in the school newsletter. If we do not have this permission, the child's photo is not used.
- Children's names should never be published where their photograph or video is being used.
- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.
- Images should be securely stored only on the school's computer system and all other copies deleted.
- Stored images should not be labelled with the child's name.
- Staff should not use personal devices to take photographs of pupils.
- Schools should inform parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.

3.5.4 Pupils own mobile phone/handheld systems

Mobile phones or other devices that allow pupils to access internet services pose a major problem for schools in that their use may distract pupils during lessons and may be used for cyber bullying.

The use of personal mobile phones or other devices **is forbidden in classrooms**.

4 Responding to Incidents

4.1 Policy statement

- All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-safety contact officer in the first instance. All incidents, whether involving pupils or staff, must be recorded by the e-safety contact officer in writing.
- Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action and consideration given to contacting the LADO where this is appropriate. Incidents involving the head teacher should be reported to the chair of the board of governors.
- The Achievement Leader should keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system.
- E-safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection teacher.

Although it is intended that e-safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Enfield can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.
- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the school's "no blame" approach.
- The incident should be reported to the e-safety contact officer and details of the website address and URL provided.
- The e-safety contact officer should liaise with the network manager or learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

4.3 Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions.
- The incident should be reported to the e-safety contact officer and details of the website address and URL recorded.
- The e-safety contact officer should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.

- The pupil's parents should be notified of the incident and what action will be taken.

4.4 Inappropriate use of IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they should report this to the head teacher and the e-safety contact officer immediately. If the misconduct involves the head teacher or governor, the matter should be reported to the chair of the board of governors.
- The e-safety contact officer will notify the network manager so that the computer, laptop or other device is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the e-safety incident report form.
- The e-safety contact officer will arrange with the network manager or learning platform provider to carry out an audit of use to establish which user is responsible and the details of materials accessed.
- Once the facts are established, the head teacher will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.
- If the materials viewed are illegal in nature the head teacher or governor should report the incident to the police and follow their advice.

4.5 Cyberbullying

4.5.1 Definition and description

Cyberbullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- School anti-bullying and behaviour policies and acceptable use policies should cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.
- Any incidents of cyber bullying should be reported to the Achievement Leader who will record the incident and ensure that the incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.
- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.
- As part of e-safety awareness and education, pupils are reminded about the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.
- Pupils are taught:
    - to only give out mobile phone numbers and email addresses to people they trust
    - to only allow close friends whom they trust to have access to their social networking page
    - not to send or post inappropriate images of themselves
    - not to respond to offensive messages
    - to report the matter to their parents and teacher immediately.
- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the pupil as evidence.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The pupil should also consider changing their phone number.
- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The pupil should also consider changing email address.
- Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.
- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.
- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

4.5.4 Cyberbullying of teachers

- We are fully aware that teachers may become victims of cyberbullying by pupils. Because of the duty of care owed to staff, the headteacher ensures that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils.
- The issue of cyberbullying of teachers is incorporated into the school's anti-bullying policy and our IT education programme, so that pupils are aware of their

own responsibilities.

- Incidents of cyber bullying involving teachers are recorded and monitored by the e-safety contact officer in the same manner as incidents involving pupils.
- Teachers should follow the guidance on safe IT use in section 3.4 of this policy and avoid using their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.
- Personal contact details for teachers should not be posted on the school website or in any other school publication.
- Teachers should follow the advice above on cyberbullying of pupils and not reply to messages but report the incident to the head teacher immediately.

4.6 Risk from inappropriate contacts and non-contact sexual abuse

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

- All concerns around inappropriate contacts should be reported to the Achievement Leader and the designated child protection teacher.
- The designated child protection teacher should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Family Services and Social Work and/or the police.
- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.
- The designated child protection teacher can seek advice on possible courses of action from Enfield's e-safety officer in Family Services and Social Work.
- Teachers will advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.
- The designated child protection teacher and the e-safety contact officer should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.
- Where inappropriate contacts have taken place using school IT equipment or networks, the e-safety contact officer should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.7 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Staff need to be aware of those pupils who are being targeted by or exposed to harmful influences from violent extremists via the internet. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.
- The school does its best to ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.
- All incidents are dealt with as a breach of the acceptable use policies and the

school's behaviour and staff disciplinary procedures are used as appropriate.

- The Achievement Leader and the designated child protection teacher should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.
- If there is evidence that the pupil is becoming deeply enmeshed in the extremist narrative, the schools will seek advice from the local authority on accessing programmes that prevent radicalisation.

4.8 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- The school gives pupils the opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum, through the SEN department, CAMHS and the Catholic Children's Society
- Pastoral support is available to all pupils to discuss issues affecting them and to establish whether their online activities are an added risk factor
- Staff receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

5. Sanctions for Misuse of School IT

5.1 Sanctions for pupils

Infringements of the Acceptable Use Policy include:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.
- continued use of non-educational or prohibited sites during lessons
- continued unauthorised use of email, mobile phones or social networking sites during lessons
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.
- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- cyber bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.
- persistent and/or extreme cyber bullying
- deliberately accessing, downloading or disseminating any material deemed

offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions for such breaches include:

- referral to Headteacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer

5.2 Sanctions for staff

Infringements of the Acceptable Use Policy include

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (eg: removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.
- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions for such breaches include:

- referral to the Headteacher
- removal of equipment
- referral to the police
- suspension pending investigation
- disciplinary action in line with school policies.

ARRANGEMENTS FOR MONITORING AND EVALUATION:	
DATE ESTABLISHED BY GOVERNING BODY:	**JANUARY 2009**
DATE REVIEWED:	**May 2015**
DATE OF NEXT REVIEW:	**TBC**
RESPONSIBILITY:	**DHT**

Appendix 1

STUDENT'S ACCEPTABLE USER POLICY

Name: ………………………………………………………… Form: …….

Keeping safe: stop, think, before you click!
12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I am aware that a member of the Strategic Leadership Team or ICT Team can view my computer screen at any time without me knowing about it.
- I am aware that I should not expect that my work and emails would always be private.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Student signature: ____ Date: ___/___/___

PARENTS/CARERS

□ I have read the above school rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.

□ I agree that my child's work can be published on the school website.

□ I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.

Parent/Carer signature: _________________________________ Date: ___/___/___

Appendix 2

ACCEPTABLE USE POLICY FOR STAFF AND GOVERNORS

Access and professional use

- All computer networks and systems belong to the school and are made available to staff and governors for educational, professional, administrative and governance purposes only.
- Staff and governors are expected to abide by all school e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken against staff or governors being removed.
- The school reserves the right to monitor internet activity and examine and delete files from the school's system.
- Staff and governors have a responsibility to safeguard pupils in their use of the internet and reporting all e-safety concerns to the e-safety contact officer.
- Copyright and intellectual property rights in relation to materials used from the internet must be respected.
- E-mails and other written communications must be carefully written and polite in tone and nature.
- Anonymous messages and the forwarding of chain letters are not permitted.
- Staff and governors will have access to the internet as agreed by the school but will take care not to allow pupils to use their logon to search the internet.

Data protection and system security

- Staff and governors should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.
- Use of any portable media such as USB sticks or CD-ROMS is permitted where virus checks can be implemented on the school ICT system using anti-virus.
- Downloading executable files or unapproved system utilities will not be allowed and all files held on the school ICT system will be regularly checked.
- Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.
- Files should be saved, stored and deleted in line with the school policy.

Personal use

- Staff and governors should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.
- Staff and governors should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.
- Staff and governors should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.
- School ICT systems may not be used for private purposes without permission from the head teacher.
- Use of school ICT systems for financial gain, gambling, political purposes or advertising is not permitted.

I have read the above policy and agree to abide by its terms.

Name: ________________________________ **Signed:** __________________________________

Date: __________________