Swallowtail Federation of Church Schools

School E-Safety Policy

All of our schools have e-Safety Coordinator. This will be the Designated Child Protection Coordinator:

Ms Nutbeam (supported by Mrs Hampshire and Mrs Mayhew) as the roles overlap at Hickling School.

Ms Nutbeam supported by Mrs Butcher at Catfield.

Ms Nutbeam supported by the Ms Wones at Sutton School.

E-safety is also monitored by Mark Sutherland, ICT technician.

- Our e-Safety Policy has been written by the school, building on the NCC e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.

How can we safely use the internet to enhance learning?

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the needs of the curriculum.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate internet content?

The schools will endeavour to ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Managing Information Systems

How will information systems security be maintained?

ICT security is a complex matter and cannot be dealt with adequately in this document. A number of agencies can advise on security including the ICT technician and ICT Solutions.

Local Area Network security issues include:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. Breaching the ICT Acceptable Use policy may result in disciplinary action.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted where possible.
- The server operating system must be secured and kept up to date.
- Virus and Spyware protection will be installed and updated regularly.
- Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security issues include:

- All Internet connections must be arranged via the Norfolk County Council Children's services to ensure compliance with the security policy.
- NCC firewalls and switches are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership basis between school and NCC.

The security of the school information systems will be reviewed regularly by the e-Safety coordinator

Virus and Spyware protection will be installed and updated regularly.

Security strategies will be discussed with ICT Solutions and ICT technician.

Login details must not be shared

- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not used without specific permission followed by a virus scan.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- The ICT technician / network manager will review system capacity regularly.

How will e-mail be managed?

Users may only use approved e-mail accounts.

Users must immediately tell a teacher if they receive offensive e-mail.

Users must not send jokes or other materials that the receiver may find offensive

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Access in school to external personal e-mail accounts should be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Email subscriptions to websites or other electronic services is not authorised.

How will published content be managed?

The school website celebrates pupils' work, promotes the school and publishes projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Publication of information should be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.

- E-mail addresses should be published carefully, to avoid spam harvesting by web crawlers
- The class teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

Images of a pupil should not be published without the parent's or carer's written permission. We ask permission to publish images of work or appropriate personal photographs once per year.

Pupils also need to be taught the reasons for caution in publishing personal information and images in social publishing sites

Images that include pupils will be selected carefully/appropriately according to parental consent.

Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

How will social networking and personal publishing be managed?

The schools will have the option to block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Pupils and staff will be advised never to give out personal details of any kind which may identify themselves or others and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Users should be advised to place only appropriate photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

Teachers' official blogs or wikis should be password protected and run from the school website.

Teachers must not run social network spaces for student use on a personal basis' - 'However professional use may be encouraged if specific to a dedicated learning outcome i.e. utilising social networking technology to provide additional support to students with their coursework. If doing so teachers need to ensure that pupils also create a 'professional' space for this purpose only

All users should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Users should be encouraged to invite known friends only and deny access to others.

Users should be advised not to publish specific and detailed private thoughts.

Schools should be aware of and deal with bullying that can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy. Abusive messages may be dealt with under the school bullying policy.

How will filtering be managed?

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- Dynamic filtering examines web page content or e-mail for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content.
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.

The Norfolk Schools Broadband Network uses a centrally managed system for both Primary and Secondary school filtering.

The school will work with ICT Solutions to ensure that systems to protect pupils are reviewed and improved.

The Headteacher will be made aware of filtering profile changes by ICT Solutions

If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator and / or ICT Solutions.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later) and ICT Solutions.

How will videoconferencing be managed?

Currently video conferring does not occur and has not been planned. If it were to occur, the following would apply:

The equipment and network

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.

External IP addresses should not be made available to other sites.

Videoconferencing contact information must not be put on the school Website.

The equipment must be secure and if necessary locked away when not in use.

School videoconferencing equipment must not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing must be supervised appropriately for the pupils' age.

Parents and guardians must agree for their children to take part in videoconferences at least in the annual return.

Responsibility for the use of the videoconferencing equipment outside school needs to be established using a risk assessment for the users.

Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.

Unique log on and password details for access to JANET / UKERNA videoconferencing services should only be issued to members of staff and kept secure (if you are using the National Education Network).

Content

- When recording a videoconference lesson, permission should be given by all sites. The reason for the recording should be given and the recording of videoconference made clear to all parties by the start of the conference.
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

Person mobile phones may not be used as part of lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden and may be illegal.

Staff will be issued with a school phone if contact with pupils is required.

Staff personal phones may be used to maintain staff to staff contact on school visits but may not be used for photographing, or accessing social networking sites.

If contact with pupils is necessary staff must use school-owned equipment.

The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy. Abusive messages may be dealt with under the school bullying policy.

How can emerging technologies be managed?

Emerging technologies will be assessed for educational benefit and a risk assessment will be carried out before use in school is allowed.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly.

NCC Data Protection information may be seen at:

Norfolk schools web site

http://schools.norfolk.gov.uk/

Commissioner's Office:

http://www.ico.gov.uk/

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff must be familiar with and sign the 'ICT Acceptable Use policy'.

Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

How will e-safety complaints be handled?

Parents, teachers and pupils should know how to submit a complaint. The facts of the case will need to be established, for instance whether the internet use was within or outside school.

Where necessary the complaints policy and disciplinary procedures will be followed.

.

How the internet is used by the school in the community

Students with outside access (e.g. on work experience) need to follow both the school's ICT Acceptable Use policy and the ICT E-safety policy and any other policies applicable to the placement.

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How the Internet is used by the community in the school

Community users coming into schools need to follow both the school's ICT Acceptable Use policy and the ICT E-safety policy and any other policies applicable to the placement.

Communications Policy

How will the policy be introduced to pupils?

E-safety is raised regularly by staff to ensure that children are e-safety aware and are familiar with the rules governing internet use within and outside of school.

The pupil and parent agreement form should be attached to a copy of the e-safety rules appropriate to the age of the pupil.

Consideration must be given as to the curriculum place for teaching e-safety. Useful e-safety programmes include:

- East of England Broadband Consortium http://www.e2bn.org/esafety
- Grid Club www.gridclub.com
- The BBC's ChatGuide: www.bbc.co.uk/chatguide/

E-Safety rules will be posted in rooms with Internet access.

Users will be informed that network and Internet use will be monitored.

The Headteacher must ensure that an appropriate person attends an e-safety training programme to raise the awareness and importance of safe and responsible internet use.

- Instruction in responsible and safe use should precede Internet access.

How will the policy be discussed with staff?

All staff will be given the School e-Safety Policy and its application and importance explained. They will be asked to sign the policy to ensure that they adhere to it.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

How will parents' support be enlisted?

Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in section 3.0 e-Safety Contacts and References.

Agreed by staff: ……. Date: Reviewed - July 2015

Agreed by Governors: …… date:

Review date: Sept 2016