Earsham
CE VA Primary School

We aim to provide a happy, purposeful, Christian environment, in which each child feels secure and develops self-confidence, enabling them to flourish and reach their full potential.
Children's learning journeys are enhanced by working together with the wider community.

E Safety

&

ICT POLICY

Staff to sign every September to say they have read policy. List in staff room.

Review summer 2019

The member of staff who has an overview of E-safety is Mr Luke Adams. He is supported by SDP Mrs S Armstrong and SDP Mrs M Mitson.

Our E-safety Policy has been written by the school, using best practice and government guidance. We have used the Norfolk Example and must acknowledge Central Primary School' E-safety Policy. It has been agreed by senior management and approved by governors.

The E-safety Policy and its implementation will be reviewed annually. The

The E-safety Policy was revised by: Sue Armstrong/Luke Adams

It was approved by the Governors on:16th July 2018, it was reported that it had been reviewed as was circulated to all staff following the meeting.

A log will be kept in the staff room to show that the policy has been read and staff will sign to confirm that they agree and follow policy procedure.

Governor minutes will confirm that governors have read and agreed the policy.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

- Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:
- Websites
- Email
- Video Broadcasting
- Podcasting
- Music Downloading
- Learning Platforms and Virtual Learning Environments
- Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Gaming and online gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality e.g. kindle Fire/ IPads

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Earsham CE VA Primary School we understand the responsibility to educate our pupils on e - safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, IPads, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc).

Roles and Responsibilities

Children's rights: Children's responsibilities:

To be able to use the internet (and email) as a means to facilitate their education and learning.

- To be protected through a filtered version of the internet
- To report anything on the internet that is inappropriate
- To be able to report anything inappropriate to members of school staff
- To be protected from cyber bullying
- To use the internet and email as directed in a safe manner
- To use appropriate security settings and to never request to befriend members of school staff on social networking sites.

Staff rights: Staff responsibilities:

- To be able to use the internet and email as a means to facilitate their teaching
- To use the internet and email in a professional and safe manner
- To be protected through a filtered version of the internet
- To report anything that is inappropriate
- To have a designated e-safety staff member
- To report anything inappropriate to the designated e-safety staff member
- To be protected from cyber bullying or online harassments
- To use appropriate security settings and
- To never befriend pupils, former pupils or their parents and carers on social networking sites

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is Mr Luke Adams. All members of the school community have been made aware of who holds this post.
It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Norfolk LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.
Senior Management and Governors are updated by the Head/e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

Governor rights: Governor responsibilities:

- To be able to use the internet and email as a means to facilitate their governor role
- To use the internet and email in a professional and safe manner
- To be protected through a filtered version of the internet
- To report anything that is inappropriate
- To know the school has a designated e-safety staff member
- To report anything inappropriate to the designated e-safety staff member
- To be protected from cyber bullying or online harassments
- To ensure that staff and pupils are following the e-safety policy

This policy, supported by the school's acceptable user agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is ICT Policy linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of Insets where applicable, presentations, email or personal notification.
- All new staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart appendix B.)
- All staff incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

The school provides opportunities within a range of curriculum areas to teach about e-Safety including using CEOP materials in all year groups. Every second year the school has a day where the children in year 5/6 learn about E Safety and Cyberbullying through a "Play in a Day" which is also shared with parents and members of the community. Every year the year 6 attend crucial crew.

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum using CEOP materials.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- From EYFS throughout the school good practice is modelled by all staff.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone.
In Foundation and KS1 the pupils have a class log in and do not use individual passwords. In KS2 pupils have individual user names.
Pupils do not use passwords but have their own log in to access their saved documents.
Staff and pupils are regularly reminded of the need for password security.
Year 5 and 6 have access to their school email addresses to access e-books via Norfolk County Council.

All users read and sign an Acceptable User Agreement to demonstrate that they have understood the school's e-safety Policy.

- Pupils are not allowed to deliberately access on-line materials, or files on the school network of their peers, teachers or anybody else without permission.
- Pupils cannot gain access to the Public drive on the server where staff save files.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks.

Individual staff users must also make sure that computers are not left unattended and are locked if they have accessed the Staff area of the Public drive.
(Ctrl ALT Delete button will enable staff to lock)

- In our school, staff use passwords to access their personal laptop and personal e-mail. All ICT passwords are the responsibility of the headteacher/designated e-safety staff member/ICT technician and all staff and pupils are expected to comply with the policies at all times.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school has implemented the new elements of data protection associated with the General Data Protection Regulation May (GDPR ,2018) and associated data protection bill.

Staff are aware of their responsibility when accessing school data. Level of access is determined by the HT.

Managing Internet Access Information
system security

School ICT systems security will be reviewed regularly (by ICT Support Provider). Virus

protection will be updated regularly (by ICT Support Provider).

Security strategies will be discussed with the Local Authority and ICT Support Provider.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

- All searching of Images is to go through via Norfolk's Firewall. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the designated e-safety staff member.

- It is the responsibility of the school, by delegation to our ICT Support Provider, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor has the network manager to install or maintain virus protection on personal systems.

If pupils wish to bring in work on removable media it must be given to the class teacher for a safety check first.

Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the headteacher.

If there are any issues related to viruses or anti-virus software, the ICT Support Provider should be informed through the log system in place in school.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. We use CEOP materials to support this.

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- At upper KS2 pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online. Such teaching is more detailed in Years 5 and 6 prior to moving onto secondary school.

Local CPO's are asked to give an informative talk relating to Internet and mobile technology use.

- Pupils are always reminded to avoid giving out personal details on the internet which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are asked to report any incidents of bullying to the school.
- Staff are totally discouraged from creating blogs to communicate with pupils. They are also clear on their professional roles with regards to social networking websites.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones) Please also see separate Mobile phone Policy

- The school allows staff to bring in personal mobile phones and devices for their own use.
- The school does not allow a member of staff to contact a pupil or parent/carer using their personal device. All contact should be conducted through the school phone & texting system.
- Exceptional circumstances may arise during a residential trip or off site visit where contact would be sanctioned by the Head Teacher.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to

understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

This is covered at Earsham Primary (n-six).

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform (the e-Safety co-ordinator/line manager) if they receive an offensive e-mail.

Safe Use of Images Taking

of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam i.e. school performances and photo sharing from residential trip
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, eg local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting pupil work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. (Appendix A)

Storage of Images

- Images/ films of children are stored on the school's network and cameras.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network
- Class teachers have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.
- Each year group has its very own USB stick to store photographs from the year which move up continually until they leave in Year 6.

Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams may be used in school for movie making only.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

Video Conferencing

- The school is not currently involved in video conferencing

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the Norfolk Flowchart for Response to an Incident of Concern will be followed.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct by training through INSET & or email reminders when and where appropriate.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school. We consult and discuss e-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website)

The school disseminates information to parents relating to e-Safety where appropriate in the form of;

- Posters e.g. CEOP materials
- Website
- Newsletter items

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

- Staff/Governors and pupils have been involved in making/reviewing the e Safety/ICT policy through staff & school council meetings.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety/ICT coordinator any issue of e-Safety that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Notes:

ICT Support Provider: Norfolk ICT Solutions
The member of staff who has an overview of E-safety is Mr Luke Adams he supported by
SDP Mrs S Armstrong and SDP Mrs M Mitson.

Related Policies

General Data Protection Regulations (GDPR ,May 2018) All relevant policies can be found in folder in policy section on the school website, hard copies can be obtained from the school office.

Spiritual, Moral, Social and Cultural Development Policy aims to prepare all pupils for the opportunities, responsibilities and expectations of life.

The Single Equality Scheme states that inclusion for all pupils will be achieved by ensuring the learning environment, resources and activities are appropriate to each child. All staff are committed to inclusion and plan lessons that dispel stereotypical attitudes and discrimination.

The Health and Safety Policy is adhered to in everything we do. The learning environment, resources and activities are planned by staff to take account of this. Children are encouraged to be safety conscious and contribute to the risk assessment process themselves.

The Special Educational Needs Policy stipulates that pupils will be assessed and provided or as an integral part of every lesson. Staff are experienced in effective differentiation and provide opportunities for children to work on their Individual Education Plan targets in all areas of the curriculum.

The Gifted and Talented Pupil Policy ensures that children who are on the register are encouraged to reach their potential through extension activities and problem solving challenges.

Mobile phone Policy Camera mobile phones are becoming increasingly popular and a built in digital camera enables users to take high resolution pictures. These can be sent instantly to other mobile phone users or email addresses. They can also be posted on the internet or in chat rooms.There is a potential for camera mobile phones to be misused in schools. They can become an instrument of bullying or harassment directed against pupils or/and teachers.

Prevention of Extremism and Radicalisation -This policy sets out our strategies and procedures to protect vulnerable pupils from being radicalised or exposed to extremist views. The elements of our policy are prevention, protection and support.

Whole School Safeguarding and Child protection Policy

The purpose of Earsham C.E. V.A. Primary School's safeguarding policy is to ensure every child who is a registered pupil at our school is safe and protected from harm. This means we will always work to;

- Protect our children / young people from maltreatment
- Prevent impairment of our children's / young people's health or development
- Ensure that our children / young people grow up in circumstances consistent with the provision of safe and effective care
- Undertake that role so as to enable our children/young people to have optimum life chances and enter adulthood successfully.

Behaviour Policy

At Earsham we believe that helping children develop attitudes that will enable them to become kind, responsible, hardworking citizens is our most far-reaching role. We create overt opportunities for development of their self esteem and work with parents to ensure children grow up with a positive sense of self worth, aware of their rights and responsibilities in a community.

Anti-bullying Policy Earsham C.E. V.A. Primary School will not tolerate any form of bullying. We believe that pupils and staff have the right to learn in an affirming and safe environment which promotes positive personal growth and self-esteem for all.

School Road, Earsham, Bungay, Suffolk NR35 2TF

Tel: 01986 892557 Fax: 01986 893634

e-mail: office@earsham.norfolk.sch.uk

www.earsham.norfolk.sch.uk

Headteacher: Mrs Sue Armstrong

Appendix A

Dear Parent/Guardian ,

Images - Consent

During the course of the school year there may be opportunities to publicise some of the activities that your child is involved in. This may well involve filming or photographing children for use in the local media. As a school, we welcome these opportunities and hope that you do too. There may also be occasions when we arrange photography for our own purposes, such as displays and school brochures.

Photography or filming will only take place with the permission of the head teacher, and under the supervision of a teacher. When filming or photography is carried out by the news media, children will only be named if there is a particular reason to do so (eg they have won a prize), and home and email addresses will never be given out.

We believe that positive publicity benefits all involved with the school. Nevertheless, we will not involve your child without your consent. Could you please take a few minutes to fill in the form overleaf and return it to the school office. Images of your child held by the school can be viewed upon request.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Videoing of special events such as sports days, plays and Christmas concerts is permitted providing that it is done by an adult known to the staff and is not shared via social media ie. Facebook etc. If any unknown adult is seen videoing or photographing children, they will be stopped immediately.

There may be other circumstances, falling outside the normal day to day activities of the school, in which pictures of children are requested. The school recognises that in such circumstances specific consent from a parent or guardian will be required before the school can permit photography or filming of children.

Yours sincerely

S Armstrong

Mrs Sue Armstrong
Headteacher

Name of child (Block Capitals):	Appendix A
Names of people responsible for the child:	1. …… 2. ……

I/We understand that images may be taken of my/our child for use as follows:

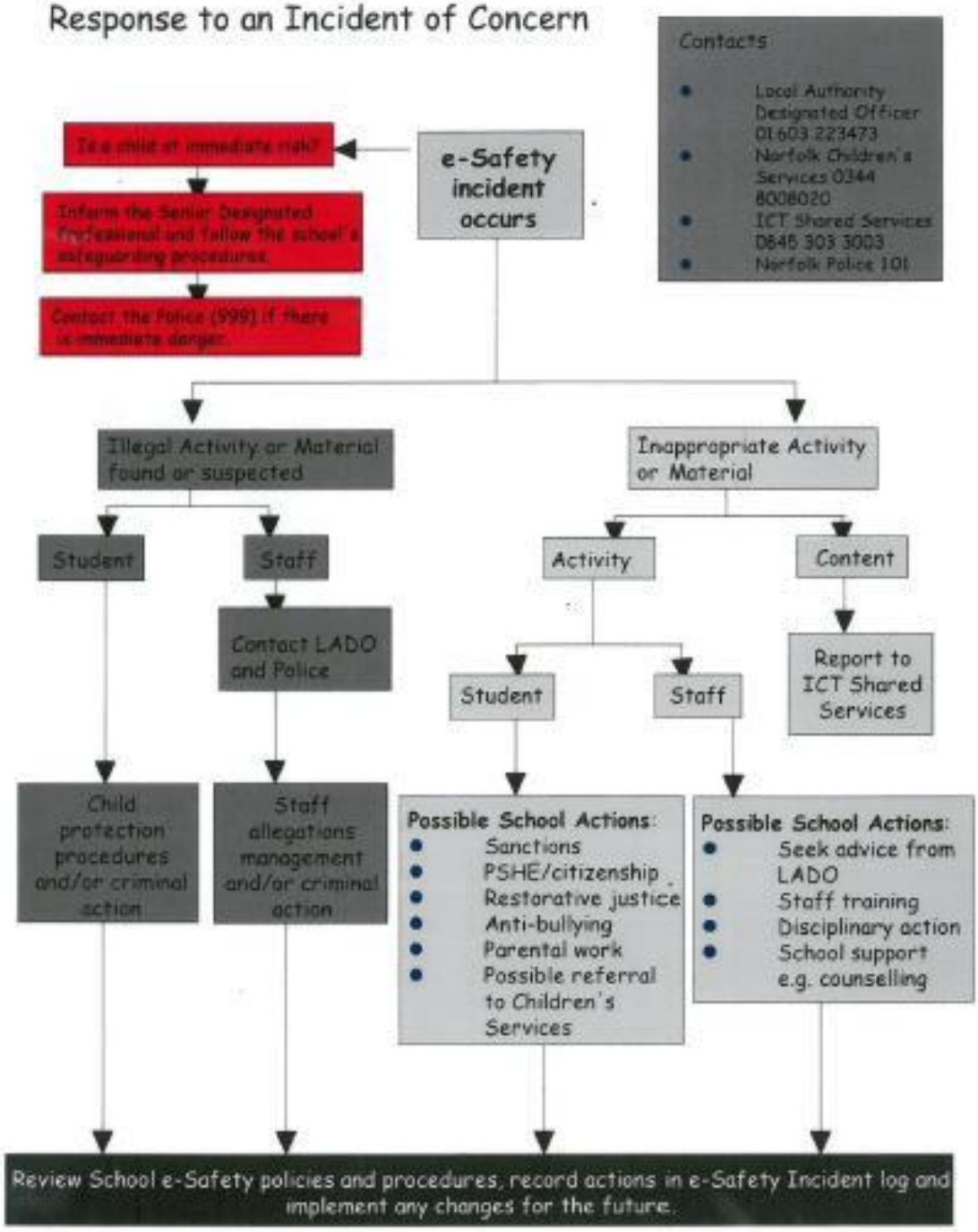
- on the school web site
- In printed publications that the school may produce for promotional purposes
- recorded/transmitted on a video or webcam i.e. school performances and photo sharing from residential trip
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Having read the statement above, do you understand how photographs will be used and give your consent for photographs or other images to be taken and used? (please tick the appropriate box)		**YES**, I give my consent for pictures to be taken and used
		NO, I do not give my consent for pictures to be taken and used
Signature/s of people responsible for the child:	1. …… Relationship to the Child: …… Date: …… 2. …… Relationship to the Child: …… Date: ……	

Appendix B

Norfolk County Council

Response to an Incident of Concern



LADO - Local Authority Designated Officer

Appendix C

EARSHAM C E V A PRIMARY SCHOOL

Responsible Internet Use

Please complete and return this form to your child's class teacher.

Pupil _____ **Class** _____

****

Pupil's Agreement

I have read and understood the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.
I understand that if I break these rules then I may not be allowed to use the Internet.

Pupil's signature _____ **Date** _____

****

Parent's/Guardian's Consent for Internet Access

I have read and understood the school rules for Responsible Internet Use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I understand that the school will not be liable for any damages arising from the use of Internet facilities.

Pupil _____ **Class** _____

Parent's/Guardian's signature _____ **Date** _____

****

Parents Consent for Web Publication of Work and Photographs

I agree that if selected, my son's or daughter's work may be published on the school website, using only their first name. I also understand that photographs that include my son/daughter will be published **only** if they comply with the school rules which state that photographs will not clearly identify individuals and that names will not be used.

Parent's/Guardian's signature_____ **Date**_____

****

SCHOOL

The school acknowledges the above signatures and therefore grants internet access

Signed _____**(Headteacher)**

WE PROMOTE STAFF WELL-BEING

fmss Financial Management Standard in Schools

ACTIVEMARK 2008

Healthy School

EARSHAM C E V A PRIMARY SCHOOL

Rules for Responsible Internet Use

The following rules apply to *all* pupils:

- I will only use the internet when supervised by a member of staff.
- I will ask permission before entering any website, unless a member of staff has already approved that site, and will only access sites that are appropriate for use in school.
- I will not give out any personal information about myself or other people (including my surname, address and telephone number).
- I will not access, send or display any offensive messages, language or pictures.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a member of staff immediately.
- I will only e-mail people whom a member of staff has approved.
- I will always ask permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will ask permission before I download or print any files.
- I will not load any disks that do not belong to the school onto any of the school's computers, as to do so may risk the introduction of viruses.
- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers in school.