E-Safety Policy

FOR
ELMHURST SCHOOL AND 2 YEAR OLD PROVISION

Adopted:	June 2015
Next Review Date:	June 2018
Responsible Committee	Premises, Health & Safety Committee

Signed:

Two Year Registered Person:	Mrs K. Rumble
Headteacher:	Mrs R. Lee
Chair of Governors:	Dr D. Gamble

E-Safety Policy

Elmhurst School is an inclusive school in the heart of Aylesbury. We continually make a positive difference to the quality of learning for all our pupils and are focused on giving all children the best possible opportunities to ensure they achieve well, enjoy school and love to learn.

Life at Elmhurst reflects our determination to secure the best possible learning outcomes for all. We take every opportunity to celebrate success whilst also ensuring that our children are happy and learn the skills and values to become successful citizens of the future. At Elmhurst each pupil is known and cared about as an individual and we set very high standards for behaviour. We have a dedicated team of staff who work hard to support our families.

Aims and Objectives

At Elmhurst we understand the Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by the school contract with Bucks County Council and Updata and includes appropriate filtering to ensure our children are safe online.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use, SMART rules are displayed around the school.
- Pupils will be educated in the effective us of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- The school will seek to ensure that the use of Internet derived materials by staff and by 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 wills be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon, immediately to their teacher/parent.

Managing Internet Access

Information System Security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.

Email

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils and staff must immediately tell a teacher or the Designated Safeguarding Lead if they receive offensive email.
- Pupils must not reveal personal details of themselves or others, or confidential information about school in email communication, or arrange to meet anyone without specific permission from a parent or carer.
- Staff must not reveal personal details of themselves or others, or confidential information about school in email communication, websites (including social networking sites) or in chat rooms.
- Staff to pupil email communication must only take place via a school email address and will be monitored. Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how email from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Remote Access

- All teachers should access emails and documents including photographs and videos via the school remote access and shared drives.

Published Content and the School Website

- The contact details on the website should be the school address, e mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupil's Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils' full names will be avoided on the website, including in blogs, and will not be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Parents sign a consent form when their child starts school to give permission for photographs to be shared online or in the media.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social Networking

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils will be encouraged to report any problems they encounter if using any social networking site and these will be reported by a member of staff on Behaviour Watch.

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Designated Safeguarding Lead.
- The Designated Safeguarding Lead, in conjunction with Interm IT (the School's ICT management and technical support provider) will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Care will be taken with games machines including the Nintendo Wii, Microsoft Xbox and others which have internet access which may not include filtering.
- Staff will use a school phone where contact with pupils or parents is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.
- Any personal devices which have access to school email accounts must be password protected and can be monitored by a member of senior staff if necessary.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and 2003.

Policy Decisions

Authorising Internet Access

- All staff must read and sign the 'Staff Code of Conduct for ICT' (Appendix 1) before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- Access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person working on school premises using the school network will be asked to read and adhere to a '**Visitor Notice - ICT Acceptable Use/Code of Conduct' form** (Appendix 2) before being allowed access to the Internet. Visitors to the school will be provided with a guest username and password to log on to the school network, which will allow limited access to files and programs.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BCC can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective. We complete annual E-Safety/ICT usage questionnaires.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/Designated Safeguarding Lead.
- Any complain about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be death with in accordance with school child protection procedures and reported to the Designated Safeguarding Lead via the CP and Welfare Concern section of Behaviour Watch.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community Use of the Internet

- All use of the school internet connection by community and other organisations shall be in accordance with the school E-Safety policy.

Introducing the E-Safety Policy to Pupils

- The children sign an 'Acceptable Use Policy' annually which is displayed in their classrooms (Appendix 4).
- Sanctions for inappropriate use of ICT by pupils will be dealt with using our school E-Safety Rules and Sanctions (Appendix 5).
- Appropriate elements of the E-Safety policy will be shared with pupils.
- E-Safety rules will be posted in all rooms with computer access.
- Pupils will be informed that network and internet use will be monitored.
- Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for pupils.
- Pupils will celebrate Safer Internet Day in February of each year in addition to e-safety lessons integrated into lessons throughout the year (following the curriculum).

Staff and the E-safety policy

- All staff have access to the School E-Safety Policy via the school website and its importance explained.
- 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 leaders and have clear procedures for reporting issues.
- Sanctions for inappropriate use of ICT by staff will be dealt with in line with the Disciplinary and Capability policy, with advice from the LADO where appropriate.

Enlisting Parents' Support

- Parents' and carers' attention will be drawn to the school E-Safety Policy in newsletters, the school brochure and on the school website.
- Parents and carers will from time to time be provided with additional information on E-Safety.

- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- The Designated Safeguarding Lead will deliver annual parent workshops covering e-safety to ensure parents are kept up to date.

Policies Associated with this Policy

- Social Networking Policy
- Linking Policy for Website Links
- Use of Mobile Phones, Cameras and Digital Technology Policy
- Safeguarding Policy

APPENDIX 1
Staff, Governor and Visitor
Acceptable Use Agreement / ICT Code of Conduct

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT Leader.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for any purpose not permitted by its owner.
- I will only use the school's email/Internet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that any personal devices including laptops, desktops, mobile phones and tablets which has access to professional email and documents is password protected.
- I will ensure that personal data is kept secure and is used appropriately on the school site and not taken off the school premises.
- I will not install any hardware of software without the permission of the ICT Leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity (including the use of social media sites), both in school and outside school, will not bring my professional role into disrepute.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead or Head teacher.
- I will ensure that electronic communications with pupils including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that phone calls made to parents are made on a school phone NOT on a personal device. If on a school trip or residential and a parent needs to be phoned the code '141' must be used before dialling to ensure privacy of personal phone number.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name………………………………………………………………………………

Job Title…………………………………………………………………………………

Signature……………………………………………….…..Date……………………..

Headteacher: RACHEL LEE

Signature…………………………………………………...Date………………………

APPENDIX 2
Visitor Notice - ICT Acceptable Use / Code of Conduct

All visitors who are using school 'WiFi' or school ICT equipment ('The Service') are required to read the terms and conditions, as set out in this Acceptable Use/Code of Conduct. When you sign into school or start using 'The Service', you are deemed to have read, understood and agreed to the contents of this Acceptable Use/Code of Conduct. Any concerns or clarification should be discussed immediately with the school office, and before using 'The Service'.

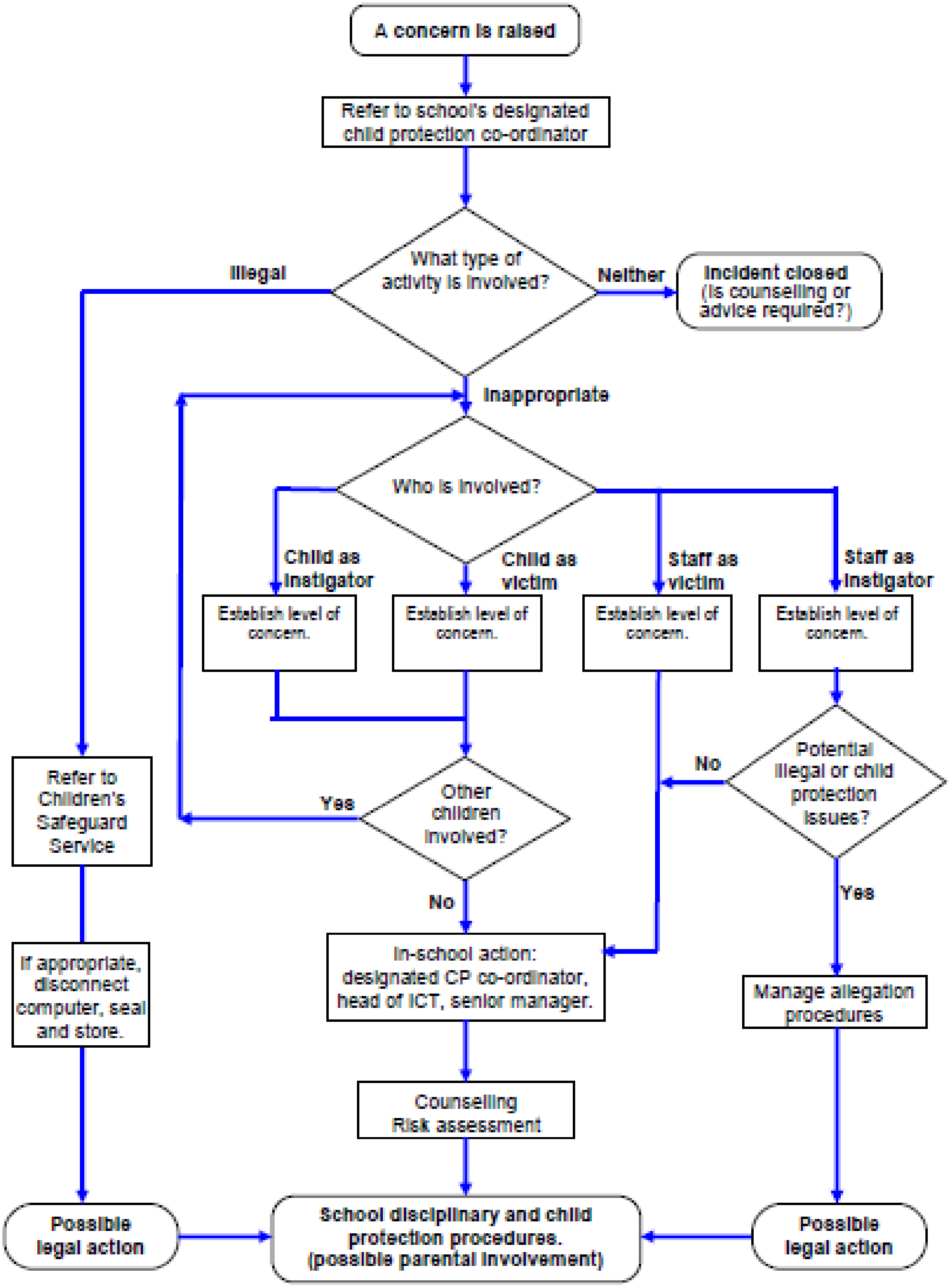
- I understand that it is a criminal offence to use a school ICT system for any purpose not permitted by its owner. I will only use the school's Internet and any related technologies for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that personal data is kept secure and is used appropriately on the school site and not taken off the school premises.
- I will not install any hardware of software without the permission of the ICT leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the ICT Leader, the Designated Safeguarding Lead or Headteacher.

APPENDIX 3

Response to an Incident of Concern

How do we respond?

The flowchart below illustrates an approach to investigating such an incident.



A concern is raised
Refer to school's designated child protection co-ordinator
What type of activity is involved?
Illegal
Neither
Incident closed (is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern.
Establish level of concern.
Establish level of concern.
Establish level of concern.
Refer to Children's Safeguard Service
Yes
Other children involved?
No
No
Potential illegal or child protection issues?
Yes
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action

Responding to an E-Safety Incident

This is guidance for senior management within schools, regarding how to respond to an E-Safety incident of concern. It is important to note that incidents may involve an adult or child as the victim or the instigator. Adults are also subject to cyber bullying by pupils.

The first section outlines key E-Safety risk behaviours. The flowchart illustrates the approach to investigating an incident of concern. This diagram should be used with the screening tool and the Buckinghamshire Safeguarding Children Board Procedures which include what to do if you are concerned about a child, or about an adult working with children. Elmhurst's DSLs will be conversant with these and the processes for referral.

They are available on the BSCB website at: http://www.bucks-lscb.org.uk/professionals/e-learning/

Further Supporting Materials are published on www.bucksgfl.org.uk and www.bucksict.org.uk

What are the E-Safety Risks?

The explosion in technology over the last 10 years, in particular the Internet, has provided endless opportunities for children, young people and adults to gain access to information and to communicate with each other. The Internet is an unmanaged, open communications channel, via which anyone can send messages discuss ideas and publish material – and it's these very features which make it an invaluable resource used by millions of children every day.

But it is these same features which present a number of risks to children. The vast majority of children's experiences will be positive - but we must be aware that this new technology can be used to bully others, and be manipulated by people who wish to do harm to children.

What does electronic communication include?

- **Internet Collaboration Tools** (e.g. social networking sites, blogs)
- **Internet Research** (e.g. web sites, search engines and Web browsers)
- **Mobile Phones and Personal Digital Assistants**
- **Internet Communications** (e.g. E-mail and Instant Messaging)
- **Webcams and Videoconferencing**

Risk Behaviours:

Online Grooming and Child Abuse

There are a number of illegal actions that adults can engage in online that put children at risk:

- Swapping child abuse images in chat areas or through instant messenger with other adults or young people and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught.
- Swapping personal information of children that they have collected with other abusers.
- Participating in online communities such as blogs, forums and chat rooms with the intention to groom children, collect sexually explicit images and meet them to have sex.

Inappropriate or Illegal Content

Because it's so easy to upload information onto the Internet, much online content is now inaccurate or extreme – yet is often presented as fact. A great deal of the material on the Internet is published for an adult audience, and some is unsuitable for children. For example, there is information on weapons, crime and racism, access to which would be much more restricted elsewhere.

Disclosing Personal Information and Identity Theft

Publishing personal information about themselves online could compromise children's security, and that of those around them. Furthermore, as soon as a message is sent or an image is posted, it can be shared, copied and changed by anyone. Children need to think carefully about their online 'etiquette'.

APPENDIX 4

Elmhurst School

Computing Rules for KS2

- Be polite (no bad or abusive language or other inappropriate behaviour).
- Keep personal information private.
- Do not post or share detailed accounts of your personal life (contact information, daily routines, location, photographs and videos).
- Do not post pictures or videos of others without their permission.
- If you see any abuse including cyberbullying, tell your teacher immediately.
- Do not click on any pop-ups (buying on-line; on-line gaming / gambling etc.).
- Do not open attachments unless you are sure the source is safe.
- Tell your teacher immediately if you see something which makes you feel uncomfortable.
- Do not respond to unkind or threatening messages (but do not to delete them, keep them as evidence of bullying).
- Do not arrange to meet anyone you have met online.

Remember the SMART Rules!

I have understood these rules and will follow them.

Signed ____

Name ____ Date ______________________

Elmhurst School

Computing Rules for Reception and KS1

I will:

- Only use the computer for what my teacher has asked me to do.
- Treat all computing equipment with respect.
- Be polite when communicating with other people.
- Keep my personal information secret.
- Tell my teacher straight away if I see something that makes me worried or upset.

Remember the SMART Rules!

I have understood these rules and will follow them.

Name ____

Date ____

APPENDIX 5

Pupil E-Safety Rules and Sanctions

It is appropriate for people to be allowed a great deal of freedom in using ICT for study, work and leisure. With freedom comes responsibility. Elmhurst School cannot control what people, all over the world, make available on the Internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form. If material is considered to be unacceptable by the school when presented in a book, magazine, video, audio tape or spoken form, then it is not acceptable on the ICT network.

We expect all ICT users to take responsibility in the following ways:

Not to access or even try to access any material which is:

- Violent or that which glorifies violence
- Criminal, terrorist or glorified criminal activity (including drug abuse)
- Racist or designed to incite racial hatred
- Of extreme political opinion
- Pornographic or with otherwise unsuitable sexual content
- Crude, profane or with otherwise unsuitable language
- Blasphemous or mocking of religious and moral beliefs and values
- In breach of the law, including copyright law, data protection, and computer misuse
- Belongs to other users of ICT systems and which they do not have explicit permission to use
- Not to search for, or use websites that bypass the school's Internet filtering
- Not to download or even try to download any software without the explicit permission of a member of the ICT systems support department
- Not to attempt to install unauthorised and unlicensed software
- To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers
- Not to use other people's user ID or password, even with their permission
- Not to interfere with or cause malicious damage to the ICT Facilities
- To report any breach (deliberate or accidental) of this policy (to the Headteacher) immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Elmhurst School reserves the right to access all material stored on its ICT system, including that held in personal areas of staff and pupil accounts for purposes of ensuring Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the ICT facilities.

Elmhurst School will act strongly against anyone whose use of ICT risks bringing the school into disrepute or risk the proper work of other users. Persistent offenders will be denied access to the ICT facilities – on a permanent basis.

Sanctions for the Misuse of Elmhurst School ICT Facilities

First Offence

- The pupil will have a conversation with the Designated Safeguarding Lead to discuss the breaking of the ICT AUP (Appendix 4).
- The pupil will need to read the ICT AUP to ensure they are clear about the expectations.
- The Designated Safeguarding Lead will write a letter to parents (or phone if required) to inform them of the breaking of the ICT AUP.
- The pupil may receive a further sanction depending on the nature of the offence.
- The relevant staff will be informed.

Second Offence

- The Designated Safeguarding Lead will write a letter to parents and phone them to inform them of the breaking of the ICT AUP (Appendix 4) for the second time. The letter may include specific information about the offence.
- The pupil may receive a further sanction depending on the nature of the offence.
- The relevant staff will be informed.

Third Offence

- The pupil will have their email and/or Internet access removed immediately by the Designated Safeguarding Lead for a minimum of 2 weeks.
- The Designated Safeguarding Lead will write a letter to parents and phone them to inform them of the breaking of the ICT AUP (Appendix 4) for the third time. The letter will ask parents to come into school to discuss the breaking of the ICT AUP with the Designated Safeguarding Lead.
- The pupil will have a meeting with the Designated Safeguarding Lead and the Headteacher to discuss the breaking of the ICT AUP and the subsequent sanction.
- The relevant staff will be informed.

Considerations will be made in line with the school behaviour and exclusion guidance where appropriate. It should be noted that if a pupil puts themselves, other pupils or a member of staff in danger by giving out personal details they will be banned from using the ICT facilities for a fixed period of time and if required the police will be informed.

APPENDIX 6

E-Safety Contacts and References

BucksICT Support Team Website
http://www.bucksict.org.uk

BucksGfL Website
http://www.bucksgfl.org.uk

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta
http://www.becta.org.uk/schools/esafety

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.Internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Stop Text Bully
www.stoptextbully.com

Think U Know website
http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/