The Crabtree Academy Trust

Crabtree Lane, Harpenden, Herts. AL5 5PU

Crabtree Infants' School
Headteacher: Mrs Sally Pattrick

Crabtree Junior School
Headteacher Mr Ian Pattrick

eSafety and ICT Acceptable Use Policy

Reference Number:	CAT012
Version	1.0
Name/Department of originator/author:	Ian & Sally Pattrick
Name/Title of responsible committee/individual:	Karen Meade, Suzanne Gaines, Phil Mercer Curriculum Sub-Committees
Date issued:	February 2017
Review frequency:	Every 3 years
Target audience:	All stakeholders

The Board of Directors shall conduct the Trust with a view to promoting high standards of learning, attainment and care.

Crabtree Academy Trust is committed to eliminating discrimination, advancing equality of opportunity and fostering good relations between different groups. These factors were considered in the formation and review of this policy and will be adhered to in its implementation and application across the whole school community.

The Crabtree Schools will promote the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs and will actively challenge any member of the school community expressing opinions contrary to fundamental British Values, including 'extremist' views.

Version	Date	Notes
V1.0	October 2015	Approved by Board of Directors
V2.0	January 2017	Updated compliance from Hertfordshire

Contents

1. Model Procedure

The Crabtree Academy Trust has adapted this policy from the Herts for Learning Model eSafety Policy issued January 2016.

2. Arrangements for Policy Monitoring and Review

Each local governing body shall appoint a named governor(s) with responsibility for ICT and eSafety.

The designated governors for ICT and eSafety are:

Crabtree Infants' School ..... Peter Phillips

Crabtree Junior School..... Nelson Hanna

Links with other policies

This policy is linked to the following Trust policies: Child Protection, Behaviour and Anti-bullying, Code of Conduct, Health and Safety, Home-School Agreement; and the schools' curriculum policies for Computing, PHSE and Citizenship.

Policy review

This policy will be reviewed at least once every three years in accordance with the Academy Trust year planner. The Policies Administrator will inform the Board of any changes to the HfL Model Policy.

3. 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
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices, including tablet and gaming devices
- Online games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

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 and that some have minimum age requirements, usually 13 years.

At The Crabtree Academy Trust, we understand the responsibility to educate our pupils on eSafety 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.

The Trust holds personal data on learners, staff and others to help them conduct their daily activities. Some of this information is sensitive and could be used by another person or criminal organization to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it difficult for the Trust to use technology to benefit learners.

Everybody in the school community, therefore, has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handlings are made aware of the risks and threats and how to minimize them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors (engaged in regulated activities) and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, *etc.*); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (*Appendices 1, 2 and 3*), is to protect the interests and safety of the whole Trust community.

4. Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The schools provide pupils with supervised access to Internet resources (where appropriate) through fixed and wireless internet connectivity.
- Staff preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- 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 are 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.
- All internet use through the HICS network is logged and the logs are randomly but regularly monitored. Whenever inappropriate use if detected, it will be followed up.

Internet Use

- It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.
- Staff must not post personal, sensitive, confidential or classified information, nor

disseminate such information in any way that may compromise the intended restricted audience.

- The names of colleagues, pupils, others or any other confidential information acquired through school must not be revealed on any social networking site or other online application.
- On-line gambling or gaming is not allowed.

Infrastructure

- Internet access at the schools is controlled through the HCC's web filtering service. For further information relating to filtering please go to **http://www.thegrid.org.uk/eservices/safety/filtered.shtml**
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- The Trust uses management control tools for controlling and monitoring workstations.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the eSafety coordinator or teacher as appropriate.
- It is the responsibility of the Trust by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Staff using personal removable media or supervising pupils using removable media are responsible for ensuring that the device is checked for viruses. It is not the Trust's responsibility, nor the network manager's, to install or maintain virus protection on personal systems.
- If a virus is suspected on any Trust ICT equipment, the user must stop using the equipment and contact Interm IT immediately, who will advise what actions to take.

Managing Other Online Technologies

Online technologies including social networking sites, if used responsibly, 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, pupils are encouraged to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the Trust endeavours to deny access to social networking and online games websites to pupils within school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher.
- Pupils are not permitted access to social media sites in school. Parents are reminded that services such as Facebook and Instagram have a 13+ age rating which they should not ignore.

5. eSafety

eSafety – Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headteachers and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named eSafety co-ordinators are Karen Meade (Crabtree Infants') / Phil Mercer and Leanne Williams (Crabtree Junior). All members of the school community have been made aware of the postholders. It is the role of the eSafety co-ordinators to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management, Directors and Governors are updated by the Headteacher/eSafety co-ordinators and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the Trust's acceptable use agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behavior/pupil discipline (including the anti-bullying) policy and PSHE.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. The Trust believes it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. The schools have a framework for teaching internet skills in Computing lessons; this is available from the ICT/Computing Subject Leader.

eSafety is embedded within the curriculum at The Crabtree Schools. The schools provide opportunities within a range of curriculum areas to teach about eSafety and we continually

look for new opportunities to promote eSafety. The following areas are addressed at the appropriate age and in an age-appropriate manner:

- Both schools have a frameworj for teaching internet skills in their computing curriculum lessons (eg. Year 6, “We are marketers” teaches children how to use search engines safely and efficiently).
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are taught about copyright, respecting other people’s information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. 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 Cybermentors, Childline or 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 Computing curriculum.

Equal Opportunities: Pupils with Additional Needs

The Trust endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools’ eSafety rules. However, staff are aware that some pupils may require additional support or 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 eSafety. Internet activities are planned and well managed for these children and young people.

eSafety Skills Development for Staff

- Staff at The Crabtree Academy Trust receive regular information and training on eSafety and how they can promote the ‘Stay Safe’ online messages. This is in the form of staff notices and business meetings as necessary (minutes distributed to all staff) and by the annual distribution of the eSafety policy, which staff must sign to say they have read.
- New staff receive information on the school’s acceptable use policy as part of their induction, and must sign the declaration. All staff are re-issued annually with the acceptable use agreement for signature.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see flowcharts in *Appendix 5*).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are kept adequately informed with up-to-date areas of concern.

Managing the School eSafety Messages

- Staff endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- Whole school eSafety messages are shared at Crabtree Infants’ School via an eSafety assembly. Crabtree Junior School has assemblies on eSafety each half term and also covers eSafety topics in PSHE lessons.

- eSafety posters are prominently displayed in every classroom.
- The key eSafety advice is promoted widely through school displays, newsletters, class activities, *etc.*
- The Trust also participates in “Safer Internet Day” every February.

Parental Involvement

The Trust believes it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. The schools provide eSafety information for parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school and also decide whether they consent to images of their child being taken and used in the public domain (*See Appendices 1, 2 and 4*).

Where appropriate, the schools disseminate information to parents relating to eSafety in the form of:

- Information evenings
- Posters
- School website and blogs
- Newsletter items

eSafety Incident Log & Infringements

A breach or suspected breach of policy by a Trust employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff, any policy breach is grounds for disciplinary action in accordance with the Trust's Disciplinary Procedure.

In incidents of breaches of policy by pupils, reference will be made to the school's behaviour policy.

Complaints

Complaints and/or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed (*see Appendix 5*)

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user is a breach of the Acceptable Use Agreement and will lead to the incident being logged by the eSafety co-ordinator and, depending on the seriousness of the offence, may result in disciplinary action.
- Users are made aware of sanctions relating to the misuse or misconduct via the Staff Disciplinary Procedures and Pupil Behaviour policy.

6. Email

The use of email is an essential means of communication for both staff and pupils/parents. 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 appropriately and how to behave responsibly online.

It should be noted that however school email is accessed (whether directly, or through webmail when away from the office or on non-school hardware) all the school email policies apply.

Pupil email

- Pupils are introduced to email as part of the Computing Programme of Study.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes; children use a class/group email address when necessary.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email.

Staff email

- The Trust gives all staff their own email account to use for all Trust and school business. This account should be the account that is used for all school business. This is to protect staff, to minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal profile information being revealed.
- Staff must check their email regularly and activate their 'out-of-office' notification when away for extended periods.
- The Trust requires a standard disclaimer to be attached to all email correspondence (Arial, font size 6):

> Before you print think about the ENVIRONMENT
>
> **Important** – This email and any attachments may be confidential. If received in error, please contact us and delete all copies. Before opening or using attachments, check them for viruses and defects. Regardless of any loss, damage or consequence, whether caused by the negligence of the sender or not, resulting directly or indirectly from the use of any attached files, our liability is limited to resupplying any affected attachments. Any representations or opinions expressed are those of the individual sender and not necessarily those of the school.

  The responsibility for adding this disclaimer lies with the account holder.
- The automatic forwarding and deletion of school emails is not allowed. Emails must be accessed via the Microsoft Office 365 account.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. Communication with parents will normally be via the School Admin address.
- It is the responsibility of each account holder to keep their password secure.
- All emails should be written and checked 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 show the correspondence to the Headteacher before sending.
- Emails created or received as part of school employment will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Staff must inform the Headteacher if they receive an offensive email.
- Attachments from an untrusted source should never be opened without first consulting the IT technician.
- School email is not to be used for personal messaging or advertising.

<u>Email management guidelines</u>

- Delete all emails of short-term value.
- Organise email into folders and carry out frequent house-keeping on all folders and archives.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not use the email systems to store attachments: business-related work should be detached and saved to the appropriate shared drive/folder on the school server.

7. Safe Use of Images

Taking of images and film

Digital images are easy to capture, reproduce and publish and, therefore, easy to misuse. 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. HCC guidance can be found at: http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

- The school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff and volunteers are not generally 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 Trust's network and deleted from the staff member's/volunteer's device.
- Pupils are not permitted to use personal digital equipment during school hours, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.
- Parents are reminded of the correct use of recordings (still or movie images) made during school performances or on other occasions, i.e. that they should focus only on their own children and recordings that include images of other children should not be uploaded to the Internet or published in any forum.

Publishing pupils' images

On a child's entry to each of the Crabtree Schools, parents/carers will be asked to give permission for the school to use their child's photograph in display or publicity material, on the school website, and in news media.

The consent form is considered valid for the entire period that the child attends the 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*. In the case of images used on the website/Blogs, the consent applies at the time the image is uploaded and therefore images may remain on the site after a pupil has left the school notwithstanding that the parent or carer may request the removal of a particular image at any time. Similarly, parents or carers may withdraw or change the general consent, in writing, at any time.

Pupils' names will only be published where consent has been given by parents (*see Appendix 3*).

Email and postal addresses of pupils will not be published.

Only the Web Managers have authority to upload images to the school websites. Teachers are responsible for ensuring that consents are in place for images uploaded to their Blogs.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see: http://www.thegrid.org.uk/schoolweb/safety/index.shtml

Storage of images

- Images/films of children are stored on the school's network. At the Junior School, archived photos are stored on a portable hard drive which is kept securely in the School Office.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- All staff have the responsibility of deleting the images when they are no longer required.
- 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.

CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Junior School Office staff and Site Manager. Notification of CCTV use is displayed at the front of the schools. Please refer to the hyperlink below for further guidance: http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

8. Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff are not permitted to access their personal social media accounts using school equipment at any time.
- Staff, governors, pupils, parents and carers are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others. Parents and pupils are reminded that the age-rating for most social media sites is 13+ and this should not be ignored.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are made aware that their online behaviour should at all times be compatible with UK law

9. ICT Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving employees of the Trust or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using Trust ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Crabtree Academy Trust

Appendix 1:

Crabtree Infants' School

Pupil Acceptable Use Agreement / eSafety Rules

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, *etc* has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school.

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address when e-mailing.
- I will only open e-mail attachments from people my teacher has approved.
- I will only open/delete my own files when my teacher tells me to.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my eSafety.

✂ ----------

Child's name: ..... Class: .....

I have discussed this with my child and he/she agrees to follow the eSafety rules and to support the safe use of ICT at The Crabtree Junior School.

In addition, as parents, we will support the Trust's approach to on-line safety and not deliberately upload to the Internet or add any text, image, sound or videos that could upset or offend any member of the Trust community or bring the Trust's name into disrepute

Parent/Carer Signature: ..... Date: .....

Name in block capitals:

Crabtree Academy Trust

Appendix 2:
Crabtree Junior School
Pupil Acceptable Use Agreement / eSafety Rules

Dear Parent/ Carer,

ICT including the internet, email and mobile technologies, *etc*. has become an important part of learning in our school. The Trust's eSafety Policy is available on the schools' websites or can be requested from either School Office.

We expect all children to be safe and responsible when using any ICT and would hope that you will apply consistent rules for Internet Access at home. In particular, we would advise that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we are aware that, in some circumstances, such sites are being used by some of our pupils and so would recommend that parents monitor this use and have access to their child's log-in and password. We would strongly advise that parents also check privacy settings to ensure that only those people who are known to their child are able to view their pages.

Please read and discuss these eSafety rules with your child and return the slip overleaf. Pupils will not be granted access to use the Internet without this signed agreement from you. If you have any concerns or would like some explanation please contact the school.

- I will only use ICT in school for school purposes.
- I will use only my own login and I will not tell other people my ICT passwords.
- I will only open/delete my own files and only when my teacher tells me to do so.
- I will only use my class email address when emailing.
- I will only e-mail people I know, or my teacher has approved and I will only open email attachments from people my teacher has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will ask permission from a member of staff before using the Internet;
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. To help protect other pupils and myself, if I accidentally find anything like this or if I receive email messages I do not like I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone, unless this is part of a school project and my parent, carer or teacher has given permission.
- I will not bring a memory stick or other portable storage or software media into school unless I have permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe. I understand that if I deliberately break the rules, I may not be allowed to use the Internet or computers.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community or bring the school into disrepute.
- I will not use personal digital equipment during school hours, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher..
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

Child's name: ..... Class: .....

I have discussed this with my child and he/she agrees to follow the eSafety rules and to support the safe use of ICT at The Crabtree Academy Trust.

In addition, as parents, we will support the Trust's approach to on-line safety and not deliberately upload to the Internet or add any text, image, sound or videos that could upset or offend any member of the Trust community or bring the Trust's name into disrepute

Parent/Carer Signature: ..... Date: .....

Name in block capitals:.....

Crabtree Academy Trust

Appendix 3:
Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This Agreement is designed to ensure Trust employees are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this Agreement annually and adhere at all times to its contents. In addition, governors and other visitors who access ICT in school or via RMPortico are asked to sign the Agreement. Any concerns or clarification should be discussed with the schools' ICT coordinators, Karen Meade (Crabtree Infants') / Suzanne Gaines and Phil Mercer (Crabtree Junior), or with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Trust.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities. Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role. The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business. I understand that I am responsible for email I send and for contacts made that may result in email being received.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software inappropriately.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. I understand that use of school IT for personal financial gain, gambling, political purposes or advertising is forbidden
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- 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 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 the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, does not bring my professional role into disrepute.
- I will support and promote the school's eSafety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- Staff only: I understand this Agreement forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct, to support the safe and secure use of ICT throughout the Crabtree Academy Trust and help pupils to be safe and responsible in their use of ICT and related technologies.

Name: ..... Role:.....

Signature ..... Date .....

Crabtree Academy Trust

Appendix 4: Image consent form

Occasionally, we take photographs of the children at The Crabtree Schools. We may use these images in the school prospectus or in other printed publications that we produce for promotional purposes; in displays that may be used in the school's communal areas or offsite; or on the Trust or school websites, learning platform or Blog pages. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

We may also send images to the news media, or our school may be visited by the media who will take their own photographs or film footage (for example, of a visiting dignitary or other high profile event). Pupils will often appear in these images. The news media may use the images in printed publications (including local or national newspapers), on televised news programmes or on their website. They then store them in their archive. They may also syndicate the photos to other media for possible use, either in printed publications, on websites, or both. When we submit photographs and information to the media, we have no control on when, where, if or how they will be used.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child.

Conditions of use:

1. This form is valid for the period of time your child attends this school. Images of your child will not be used after this time, although images uploaded during your child's time in school may remain on the school blogs or website after they have left. Please write to the school if you wish to withdraw consent at any time.
2. The images we take will be of activities that show the school and children in a positive light.
3. Embarrassing or distressing images will not be used. The images will not be associated with negative or sensitive issues.
4. We may use group or class photographs or footage with very general labels e.g. 'science lesson'.
5. We will only use images of pupils who are suitably dressed.
6. We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.
7. We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers or for any consequences arising from publication.

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies. In giving your consent you understand that images may be used in printed and electronic form.

To give your consent, please complete the information below and return the form to the school.

Please tick those that apply:

I give permission for my child's image to be used in displays in the school's communal areas or in offsite displays	☐
I give permission for my child's image to be taken and used in publicity material for the school, including printed and electronic publications (*e.g.* Prospectus), video and webcam recordings and on blogs and websites	☐
I give permission for images of my child to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent by the school to the news media and images / footage the media may take themselves if invited to the school to cover an event.	☐
In the event of photographs appearing in the news media, I give permission for my child's name and surname to be published alongside the photograph	☐
I do not want my child's image used in any publicity	☐

I have read and understood the information overleaf.

Name of child: _____

Parent's or carer's signature: _____

Name (in block capitals) _____

Date: _____

School: _____

If you require help completing this form or a translated version, please contact the School Office.

Appendix 5: Managing an eSafety Incident Flow charts

Staff, parents, children, young people, governors and others can all become involved in an eSafety incident either as an instigator or victim. To help reduce the number of incidents we suggest that all schools and governing bodies consider the following:

Ways to prevent eSafety incidents

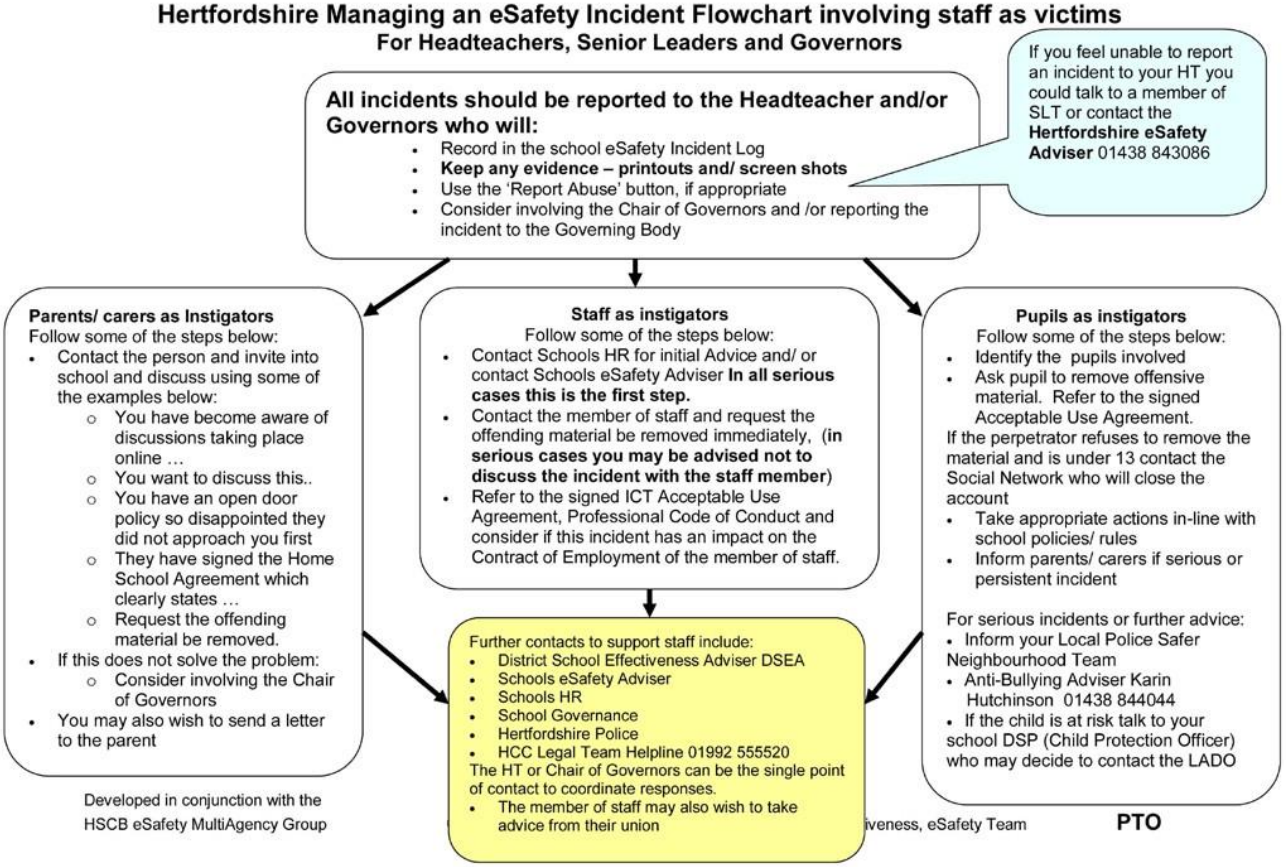
- Have up to-date ICT Acceptable use Policies for All users with signed user agreements. Sample policies can be found on the HGfL http://www.thegrid.org.uk/eservices/safety/policies.shtml
- Include a sentence in your **Home school Agreement**
  - ***We will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community'***
- Hold regular eSafety awareness/ update sessions for staff, governors, parents and carers
- Have an effective school complaints system which all parents, carers and others feel confident will address their concerns
- Embed eSafety throughout the curriculum and beyond

Developed in conjunction with the HSCB eSafety MultiAgency Group

PTO

Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and Governors



Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident

For Headteachers, Senior Leaders and eSafety Coordinators

Following an incident the eSafety Coordinator and/ or Headteacher will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact immediately for advice either:
Herts. ICT Technical Adviser
01438 844809
Youth Crime Reduction Officer
Local Safer Neighbourhood Officer

Illegal means something against the law such as:
- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

Was **illegal** material or activity found or suspected?

Yes

1. Inform police and the Herts. ICT Technical Adviser. Follow any advice given by the Police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

If a pupil is involved inform the Child Protection School Liaison Officer (CPSLO) on 01992 556936.
If a member of staff, contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 555420.

No

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to **switch off their monitor or close laptop** if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator

Hertfordshire Managing an eSafety Incident Flowchart

For Headteachers, Senior Leaders and eSafety Coordinators

If the incident **did not** involve **any illegal activity** then follow this flowchart

The eSafety Coordinator and/ or Headteacher should:
- Record in the school eSafety Incident Log
- Keep any evidence

Incident could be:
- Using another persons user name and password
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 844044

Did the incident involve a member of staff?

Yes

If member of staff has:
1. Behaved in a way that has harmed a child, or may have harmed a child.
2. Possibly committed a criminal offence against or related to a child; or
3. Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Contact the LADO on: 01992 555420
If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:
- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact school HR
  Sandie Abery 01438 843798 South-E
  Rachel Hurst 01438 843767 North-W

No

Was the child the victim or the instigator?

Pupil as victim

In –school action to support pupil by one or more of the following:
- Class teacher
- eSafety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately
Confiscate the device, if appropriate.

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to **switch off their monitor or close laptop** if they find something unpleasant or frightening and talk to a member of staff or the eSafety Coordinator

Current Legislation and Advice
Including PREVENT Guidance

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual

offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

access to computer files or software without permission (for example using another person's password to access files)

unauthorised access, as above, in order to commit a further criminal act (such as fraud)

impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services