St Columba's Catholic Primary School

ACCEPTABLE USER POLICY

Reviewed September 2019

TABLE OF CONTENTS

1. What is an AUP (Acceptable Use Policy)? 2
2. Why have an AUP? 2
3. Aims 3
4. Roles and responsibilities of the school (or establishment) 3
   - 4.1 Considering your legal powers 3
   - 4.2 Governors and Headteacher 4
   - 4.3 e-Safety Leader 4
   - 4.4 Staff or adults 5
   - 4.5 Children and young people 6
5. Appropriate use by staff or adults 7
   - 5.1 In the event of inappropriate use 7
6. Appropriate use by children and young people 7
   - 6.1 In the event of inappropriate use 8
7. The curriculum and tools for Learning 9
   - 7.1 Internet use 9
   - 7.2 Learning Platform 10
   - 7.3 E-mail use 11
   - 7.4 Mobile phones and other technologies 12
   - 7.5 Video and photographs 12
8. Filtering and safeguarding measures 13
9. Monitoring 14
10. School library 14
11. Parents 15
    - 11.1 Roles 15
    - 11.2 Support 15
12. Links to other policies 15
    - 12.1 Behaviour and Anti-Bullying Policies 15
    - 12.2 Inter Agency Safeguarding Children Procedures 16
    - 12.3 PSHE and other areas of the curriculum 16
    - 12.4 Health and Safety 16
    - 12.5 School website (if different to the Learning Platform space) 16
    - 12.6 External websites 17
    - 12.7 Disciplinary Procedure for All School Based Staff 17

APPENDICES 18

- Core AUP statements 19
- Staff Procedures Following Misuse by Staff 20
- Staff Procedures Following Misuse by Children and Young People 22
- Acceptable Use Rules for Staff 24
- Parent/Child Agreement 26
- Key Stage 1 Rules 28
- Key Stage 2 Rules 29
- Key Stage 3 and 4 Rules 30
- Secondary e- Safety awareness for students 30
- Reporting an Incident Workflow Diagram 33
- Further Information and Guidance 34

Knowsley Council
Directorate of Children & Family Services
Acceptable Use Policy

1. What is an AUP (Acceptable Use Policy)?

In accordance of the Data Protection Act 2018/GDPR - An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all on-line technologies (including the Internet, E-mail, web cams, Instant Messaging and other social networking spaces, mobile phones and games) to safeguard adults and children and young people within the school setting. It details how the school will provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies, beyond the school setting. It also explains procedures for any unacceptable behaviour or misuse of these technologies by adults or children and young people. This is also referenced within the Staff handbook.

2. Why have an AUP?

Knowsley acknowledges that transformation isn't just about buildings - our ICT Strategy is founded on four pillars:

Access:
Borough-wide connectivity to digital resources enabling learners to connect via a portable and interactive device ensuring every learner has guaranteed access to digital learning resources.

Digital Resources:
That cover all areas of the curriculum tagged in relation to Becta standards. Facilities for digital resources to be easily created and amended to encourage organic growth of learning resources.

Delivery Systems:
A Personalised Learning Environment (PLE) capable of delivering, creating and manipulating digital resources to assist in overall delivery of personalised learning. The PLE will provide full assessment and tracking features including the ability to monitor e-Attendance within the concept of anywhere, anytime, any place learning. A personalised learning space available to each student incorporating accessible storage space and email facilities that will enable the learning account to be transferable to lifelong learning institutions via an ePortfolio.

Support & Development:
Deployment of effective technical support to harness all the advantages of standardised systems and remote support, releasing staff from pursuing technical support issues in person supported by Continuous Professional Development of teachers and non-teaching staff in the use of ICT and the development of discreet resources, with consideration of the workforce remodelling cross-cutting theme. The creation.

We are committed to staff development with the emphasis on developing a workforce with skills to take educational delivery into the 21st century.

The use of the Internet and connectivity to digital resources as a tool to develop learning and understanding is now an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.

- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst the school or setting acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected.

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children Act 2004 places a duty on schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children and young people and parent/carers is also vital to the successful use of on-line technologies, so this policy also aims to inform how parents/carers and children or young people are part of the procedures and how children and young people are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect children, young people and adults from potential and known risks.

3. Aims

The Aims of this Acceptable Use Policy are:

- To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of everyone working with children and young people.
- To ensure adults are clear about procedures for dealing with misuse of any on-line technologies both within and beyond the school setting.
- To develop links with parents/carers and the wider community ensuring their input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

4. Roles and responsibilities of the school (or establishment)

4.1 Considering your legal powers

Sections 90 and 91 of the Education and Inspections Act 2006 statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. Section 94 also gives schools the power to confiscate items from pupils as a disciplinary penalty.

These powers may be particularly important when dealing with e-safety issues: we know, for example, that online bullying may take place both inside and outside school, and so this

legislation will give schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the wellbeing and safety of others. **It is important to remember that intimidation and harassment in whichever form it is delivered is a criminal offence and could result in prosecution.**

Schools should consider their legal powers when developing e-safety policies and document sanctions for breaches of policy accordingly. The DCSF has produced a short guide to help schools understand their powers under the provisions of the Act. This can be obtained at: http://www.dcsf.gov.uk/educationandinspectionsact/docs/Guide%20to%20the%20Education%20and%20Inspections%20Act.pdf

4.2 Governors and Headteacher *(To be substituted with other relevant staff as required by the establishment.)*

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher has designated an e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- *The Headteacher, along with the governors will need to decide if there should be a standard disclaimer on all e-mails stating that the views expressed are not necessarily those of the school or the LA.*
- Time and resources will be provided for the e-Safety Leader and staff to be trained and update policies, where appropriate. *Establishment to decide how much time to be allocated*.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan. As a minimum one member of staff must have undertaken the Child Exploitation and On-line Protection Centre (CEOP) Ambassador training.
- The Headteacher will inform the Governors at the Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors will be made aware of e-Safety developments from the Curriculum meetings.
- The Governors MUST ensure Child Protection requirements are met including an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- An e-Safety Governor (can be the ICT or Child Protection Governor) will challenge the school to ensure there is an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers. See appendices for example procedures on misuse.

4.3 e-Safety Leader

It is the role of the designated e-Safety Leader or Committee (*which could also be the ICT, PSHE or Child Protection Designated Person already in role but should be a senior member of the school and not a network manager*) to:

- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that, in cooperation with Information & Technologies staff, filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-alone PC, staff/children laptops and the learning platform.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis. *School to decide how frequently and whether this will be at the Governors Curriculum Meeting.*
- Liaise with the PSHE, Child Protection and ICT leads so that all policies and procedures i.e. cyberbullying etc are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies e.g. THINKUKNOW so that the correct e-safety information can be taught or adhered to.
- Liaise with Information & Technologies staff on the monitoring of the Internet and on-line technologies - determining how the school wish to monitor the use of the Internet and technologies by staff, children and young people.
- Decide the use of personal equipment in school or settings for work purposes, such as a digital camera or the use of a personal e-mail address and the procedures for using school equipment at home – signed acceptable use forms by staff need to be considered if using own equipment so that it is clear how, when, why and where equipment is used and storing/discarding of images etc…takes place. This is a key decision to make it also means all staff members are potentially more at risk of allegations being made against them if using their own equipment, especially if this is unauthorised.
    - Home use of school or setting equipment must be in keeping with this policy.
    - Personal equipment may be used at school subject to appropriate electrical testing at work and used in keeping with this policy.
- Keep a log of incidents for analysis to help inform future development and safeguarding and where risks can be identified, to ensure the correct procedures are used with incidents of misuse (website in Appendices).
- Work alongside the ICT Leader and Information & Technologies staff, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

4.4 Staff or adults

It is the responsibility of **all** adults within the school or other setting (including volunteers, consultants and contractors) to:

- Ensure that they know who the Designated Person for Child Protection is within school or other setting so that any misuse or incidents which involve a child can be

reported. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately. (Following the Inter Agency Safeguarding Children Procedures.)

- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the E-safety Leader.
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of on-line technologies and know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 2018.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- All staff including school bursars/administrators will need to ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the e-Safety Leader in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies in the same way as for other non-physical assaults.

All adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust.

4.5 Children and young people

Children and young people are:

- Involved in the review of our Acceptable Use Rules through the school council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.
- Taught to respect the equipment they use and made aware of the penalites for wilful damage.
- Taught to use the Internet across the curriculum in a safe and responsible manner through ICT, PSHE or other clubs and groups to minimise risks.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

5. Appropriate use by staff or adults

Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school or setting to keep under file with a signed copy returned to the member of staff.
The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. *Staff training should underpin the receipt of this policy.*

When accessing the Learning Platform from home, the same Acceptable Use Rules will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.
Please refer to appendices for a complete list of Acceptable Use Rules for Staff. *Decide whether these are going to be signed by staff to show acceptance.*

5.1 In the event of inappropriate use

If a member of staff is believed to misuse the Internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher immediately and the KSCB Inter agency safeguarding Children Procedures and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.
In the event of accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

6. Appropriate use by children and young people

Acceptable Use Rules and the letter for children and young people and parents/carers are outlined in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules will be on display within the classrooms and in the computer suite, where this may be applicable.

We want our parents/carers to support our rules with their child or young person, which is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting, the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.

Further to this, we hope that parents/carers will add to future amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and have appropriate copyright permission. Down loading of materials maybe vague – ITS have procedures about downloading which must be adhered to in relation to opensource software etc. The policy must take consideration of this and reference. Advide from Graham Crowder could be useful.

File-sharing via e-mail, weblogs or any other means on-line should be appropriate and have copyright clearance when using the learning platform in or beyond school.
Again – please reference Information Security Policy
The school council are actively involved in discussing the acceptable use of on-line technologies and the rules for misusing them. School needs to decide how this will work and how the rules/information will be disseminated across the school.

There is also an underlying responsibility to respect the equipment being used.

6.1 In the event of inappropriate use by adults, children and young people.

Should a child or young person be found to misuse the on-line facilities whilst at school or in a setting the following consequences will occur (these will be reviewed by school council and stakeholders as the policy is updated):

- *Establishments will need to decide here what the consequences of rule breaking will be and need to create an order of escalation of consequences for misdemeanours ranging from minor to serious (potentially involving the police). This should link to existing behaviour policies which may in the light of this policy require amendment. See the Appendix for a possible list of misuse and actions.*
  - Any child found to be misusing the Internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
  - Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
  - A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person accidentally accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

Children and young people should be taught and encouraged to consider the implications for misusing the Internet for example, posting inappropriate materials to websites via mobile phones etc, as this can lead to legal implications.

6.2 Guidance for adults and children and young people

Guidance on what we do if on the following scenarios is given as an appendix at the end of this document.

1. An inappropriate website is accessed unintentionally in school by a teacher or child.
2. An inappropriate website is accessed intentionally by a child.

3. An adult uses School IT equipment inappropriately.
4. A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.
5. Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.
6. You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

6.3 Safer Practice with Technology

Kent LTSB have produced a document in response to questions raised by adults working with children and young people, which aims to assist adults to work safely and responsibly, monitor their own standards and practice and help set clear expectations of their own behaviour in compliance with codes of practice. It provides responses to the following questions:

Q1 Should I use my mobile phone to take photographs of students?
Q2 Should I continue to use my Social Networking site?
Q3 Should I have my pupils as friends on Instant Messaging services?
Q4 What is my responsibility for the use of my school laptop at home?
Q5 What is inappropriate material?
Q6 How should I store personal data safely?
Q7 How can I use ICT appropriately to communicate with young people?
Q8 As a technician, how can I safely monitor school network use?
Q9 Can my school limit private online publishing?
Q10 How do I ensure safer online activity in the primary classroom?

If in doubt

Consult with your line manager and school policies.
Consider how an action would look to a third party.
Only publish content that you would be happy to share with parents, pupils and your employer.

7. The curriculum and tools for Learning

7.1 Internet use

We teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they leave *Year 6 or Year 11*:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

To teach Internet and E-mail lessons from Years 1 to 6, where each unit of work contains a lesson on e-safety the www.thinkuknow.co.uk resources for KS1 and KS2, within PSHE may be useful.

Key Stage 3 requires young people to learn e-Safety as part of the National Curriculum for ICT so schools will need to explain how they are addressing the needs of this aspect of the curriculum, e.g. Most pupils recognise the need to be safe and act responsibly when using digital communications.
The www.thinkuknow.co.uk resources may be used, with free training available provided to teachers/adults for the delivery of these lessons.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

Personal safety – In accordance with Daata protection Act 2018 and GDPR - ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team
- think before you post a photograph, is it necessary, does it identify other people, if so do I have their permission to post it, lock it down so it cannot be copied.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.

7.2 Learning Platform

The learning platform provides a wealth of opportunity for adults, children and young people within and beyond school to:

- access resources
- collaborate and share work
- ask questions
- debate issues
- dialogue with peers
- dialogue with family members or carers
- access resources in real time
- access other people and cultures in real time
- develop an on-line community

The tools available for use within the learning platform for adults, children and young people include:

- Internet access
- E-mail
- Weblogs (on-line diaries)
- Wikis (on-line encyclopaedia or dictionary)
- Instant Messaging
- An on-line personal space for adapting as a user to:
  - upload work
  - access calendars and diaries
  - blog

The personal space (My Site) contains some information about the user. This area should be used as an opportunity to discuss with children and young people appropriate information to enter to ANY website asking for personal details (such as a social networking site e.g. Bebo and Facebook) and should reflect key messages for any on-line use.

Children and young people should use their login and password to access the Internet via the learning platform so that the level of filtering is appropriate.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

Social networking is an excellent way to share news with family and friends. Providing the security of your profile has been set correctly and a strong password used, information should remain private. The danger is that few people understand profile privacy settings. The minimum age of use of a social networking site must be observed by a school, even though many pupils disregard this legal requirement.

7.3 E-mail use

We have E-mail addresses for children and young people to use, as a class and/or as individuals *decide as a school which are appropriate for different age groups, with a view to younger children and young people requiring support to send and receive e-mails*, as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual E-mail accounts can be traced if there is an incident of misuse whereas class E-mail accounts cannot, especially for older users.

Staff, children and young people are to use their school issued e-mail addresses for any communication between home and school only. A breach of this will be considered a misuse and will result in consequences.

Staff members must not to give out and are not allowed to use their personal email address to contact children and young people under any circumstances.

Parents/carers are encouraged to be involved with the monitoring of E-mails sent although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of E-mails where there are communications between home and school/setting, on a regular (weekly or as necessary) basis. Where an establishment has a network manager, there is an expectation that monitoring software is used to flag up inappropriate terms and that a Senior Member of the Team has an overview of potential issues on a regular basis – refer to the Monitoring section for further information.

7.4 Mobile phones and other technologies

Schools and settings should carefully consider how the use of mobile technologies can be used as a teaching and learning tool within the curriculum *and consider how they will monitor and manage this*, with the following areas of concern to be taken into consideration:

- inappropriate or bullying text messages
- images or video taken of adults or peers without permission being sought
- 'happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed
- Use of web functionality

Further guidance from the DCSF around the misuse of these technologies can be found at www.teachernet.gov.uk/publications

This also applies to other mobile technologies such as a PDA. The same rules of acceptable use will apply to mobile phone users.

Staff members are not allowed to use their personal numbers to contact children and young people under any circumstances.

It is also our policy to ensure that we educate our children and young people in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.

Other technologies schools and settings use with children and young people are:

- *photocopiers*
- *fax machines*
- *telephone*
- *PDAs*
- *iPhones*

7.5 Video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.
The establishment needs to make a decision as to whether it is appropriate for staff to use their personal mobiles or other personal equipment. If the decision is taken to allow staff to use their own equipment, then there needs to be a clear procedure for timeframes on taking and storing images to a central place on a the network. (This could be part of the signed agreement by staff.)

The personal space (My Site) on the learning platform should not have personal photographs uploaded that reveal more than a general location, an activity (without close-ups of children's or young person's faces) or piece of work, without the express permission of parents/carers and school or setting. It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of staff.

Photographs/images used to identify children and young people in a forum or using Instant Messaging will be representative of the child rather than of the child e.g. an avatar.

Particular care is required around development of school websites. Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although Child Protection Guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. School will need to decide how photographs will be used, including where they will be stored (central location which could be viewed by anyone) and when they will be deleted.

A school trip is a common situation where photography by pupils and staff should be encouraged, but there are potential dangers. The safest approach is to avoid the use of personal equipment and to use a school-provided item. One potential danger is an allegation that an adult has taken an inappropriate photograph. With a personal camera it would be more difficult for the adult to prove that this was not the case.
With school equipment there is at least a demonstration that the photography was consistent with school policy.

Care should also be taken that photographs are stored appropriately. For instance to copy the photograph on to a personal laptop as opposed to a school allocated laptop might make it difficult to retain control of how the picture is used. Memory cards, memory sticks and CD's should only provide a temporary storage medium. Once photographs are uploaded to the appropriate area of the school network images should be erased immediately from their initial storage location.

It is important to continue to celebrate achievements of pupils through the appropriate use of photography in communicating with parents and the community.

8. Filtering and safeguarding measures

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way.

The learning platform is set within a filtering service that will provide the same level of protection for all users. Within our Primary and Specialist sector Websense is the tool used.The web filtering for our Centres for Learning are part of the RM Managed Service.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis.

A corporate firewall ensures information about our children and young people and the school cannot be accessed by unauthorised users.

Children use a search engine that is age appropriate such as AskJeeveskids or Yahooligans.

Links or feeds to e-safety websites are provided.

For older children and young people, the Report Abuse button is available should there be a concern of inappropriate or malicious contact made by

someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and On-line Protection Centre) training for secondary children and young people (and Year 6 Primary children) is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible. Additional support and materials can be provided by the Local Authority via the City Learning Centres.

What is the guidance for schools in terms of safeguarding of young people online including phones? Do all schools have an esafety lead and what is the recommendation for refresher training?

9. Monitoring

Staff and children and young people should be informed that monitoring is in place.

The e-Safety Leader and/or a senior member of staff should be monitoring the use of on-line technologies by children and young people and staff, on a regular basis.

Network Managers should not have overall control of network monitoring.

Teachers monitor the use of the learning platform and the Internet during lessons and also monitor the use of e-mails between school and at home, on a regular basis.

Filtering or recording network usage will only be effective if monitored carefully to notice and report inappropriate access or usage. Often this places a new responsibility on technical staff that they may not be trained for. This responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity.

It is wrong to assume that filtering and monitoring are simply technical ICT activities, solely managed by the network staff. Some technical staff have indeed taken on this wider responsibility to help ensure that ICT use is appropriate and beneficial. However technical staff should not be expected to make judgements as to what is inappropriate material or behaviour, without support and supervision.

The monitoring policy must be set by the senior leadership team, with set procedures to deal with incidents. The senior leadership team will require assistance from technical staff, but must also involve the school designated child protection coordinator and pastoral staff.

A technician might, with the best of intent, check sites that a user has visited and email images to alert a colleague. Should the images prove to be illegal the technician has committed a criminal offence. A defence may be that the technician was acting within a published school procedure, but staff should ensure that they receive a specific, written request to perform this work.

10. School library

The computers in the school library are protected in line with the school network.

Where software is used that requires a child login, it is password protected so that the child is only able to access themselves as a user. Children and young people should be taught not to share passwords.

The same acceptable use rules apply for any staff and children and young people using this technology.

11. Parents

11.1 Roles

(There is no statutory requirement for parents to sign acceptable use policies but evidence shows that children and young people signing agreements to take responsibility for their own actions, is successful. http://www.teachers.tv/video/22517 shows an excellent example of this for bullying.)

Each child or young person will receive a copy of the Acceptable Use Rules on an annual basis or first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

School will keep a record of the signed forms.

11.2 Support

Schools and settings may choose to follow or adapt this guidance:
As part of the approach to developing e-safety awareness with children and young people, the school or setting may offer parents the opportunity to find out more about how they can support the school or setting in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond school. The school or setting may want to promote a positive attitude to using the World Wide Web and therefore want parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly.

We will use the Childnet International 'KnowITAll for Parents' CD/on-line materials (http://www.childnet-int.org.uk/kia/parents/cd/) to deliver key messages and raise awareness for parents/carers and the community. Ensure that skills around Internet use are offered as part of the follow-up training for parents/carers so they know how to use the tools their children and young people are using this will provide parents with information on how the school protects children and young people whilst using the learning platform facilities, such as the Internet and E-mail. It will also be an opportunity to explore how the school is teaching children and young people to be safe and responsible Internet users and how this can be extended to use beyond the school environment.

The Appendices detail where parents/carers can go for further support beyond the school. The school will endeavour to provide access to the Internet for parents/carers so that appropriate advice and information can be accessed where there may be no Internet at home, subject to arrangement.

12. Links to other policies

12.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. Schools should have an up to date Anti-bullying Policy which will include any cyberbullying issues. All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT and PSHE materials for children and young people and their parents/carers. People should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

12.2 Inter Agency Safeguarding Children Procedures

Please refer to the Inter Agency Safeguarding Children Procedures, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations should be reported to the Headteacher immediately or Chair of Governors in the event of the allegation made about the Headteacher.

Please refer to the Inter Agency Safeguarding Children Procedures for the correct procedure in the event of a breach of child safety and inform the designated person for child protection within school immediately.

12.3 PSHE and other areas of the curriculum

We link the teaching and learning of e-Safety with our PSHE and other curriculum areas by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people.

12.4 Health and Safety

Refer to the Health and Safety Policy and procedures of the school/setting and the Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

12.5 Safer Practice with Technology

Kent LTSB have produced a document in response to questions raised by adults working with children and young people, which aims to assist adults to work safely and responsibility, monitor their own standards and practice and help set clear expectations of their own behaviour in compliance with codes of practice. This document can be found at ”

http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/E-Safety/SaferPracticeWithTechnology-260509.pdf

12.6 School website (if different to the Learning Platform space)

The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission is always sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

12.7 External websites

In the event that a member of staff finds themselves or another adult on an external website, such as ‘Rate My Teacher’, as a victim, schools/settings are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

12.8 Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

APPENDICES

Core AUP statements

Although AUPs should reflect the local context, there are core statements or approaches which all settings are likely to want to adopt and adapt as appropriate to the end-user's age and understanding. For example:

- All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.
- No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form.
- No applications or services accessed by users may be used to bring the school, or its members, into disrepute.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.
- All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- All users should use network resources responsibly. Wasting staff effort or networked resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable.
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- All users should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.
- All users must take responsibility for reading and upholding the standards laid out in the AUP.
- All users should understand that the AUP is regularly reviewed and consistently enforced.

The AUP should also:

- provide information on where users can access material, advice and guidance relating to e-safety issues
- provide information on what sanctions may be taken if the AUP is not followed.

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. *An inappropriate website is accessed inadvertently:*

- Report website to the e-Safety Leader.
- Contact the helpdesk so that it can be added to the banned or restricted list.
- Change Local Control filters to restrict locally.
- Check the filter level is at the appropriate level for staff use in school.

B. *An inappropriate website is accessed deliberately:*

- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Headteacher and e-Safety Leader immediately.
- Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.

C. *An adult receives inappropriate material.*

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

D. *An adult has used ICT equipment inappropriately:*

- Follow the procedures for B.

E. *An adult has communicated with a child or used ICT equipment inappropriately with regard to children:*

Ensure the child is reassured and remove them from the situation immediately, if necessary.

- Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Inter Agency Safeguarding Children Procedures.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Inter Agency Safeguarding Children Procedures.
- Contact CEOP (police) as necessary.

F. *Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:*

- Preserve any evidence
- Inform the Headteacher immediately and follow Child Protection Policy as necessary.
- Inform the e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. *Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted*

- This should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. *An inappropriate website is accessed inadvertently:*
- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the e-Safety Leader if this is deemed necessary.
- Contact the helpdesk so that it can be added to the banned list or use Local Control to alter within your setting.
- Check the filter level is at the appropriate level for pupil use in school.

B. *An inappropriate website is accessed deliberately:*
- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Inform LA as above regarding filtering.

C. *An adult or child has communicated with a child or used ICT equipment inappropriately:*
- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Headteacher and Designated Person for Child Protection immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse i.e. where it appears that the incident refers to grooming or child exploitation the Headteacher must follow the Inter Agency Safeguarding Children Procedures.
- Contact the safer schools officer, local police and/or CEOP as necessary.

D. *Threatening or malicious comments are posted to the school website or learning platform about a child in school:*
- Preserve any evidence.
- Inform the Headteacher immediately.
- Inform the e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

E. *Threatening or malicious comments are posted on external websites about an adult in the school or setting:*
- Preserve any evidence.
- Inform the Headteacher immediately.

N.B: **There are three incidences when you must report directly to the police as well as the Headteacher and e-Safety Leader.**

- **Indecent images of children found.**
- **Incidents of 'grooming' behaviour.**
- **The sending of obscene materials to a child.**

CEOP advice is to

- turn off the screen;
- secure the machine; and
- contact the police for further instructions if an indecent image is found.

They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. **If in doubt, do not power down the machine.**

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

- www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Knowsley Inter Agency Safeguarding Children Procedures need to be followed by the school.

All adults should know who the Designated Person for Child Protection is.

It is important to remember that any **offensive images that may be received should never be forwarded to anyone else,** even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 2018 and GDPR and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password or other security information I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed…….Date…….

Name (printed)…….

School……...

Parent/Child Agreement

e-Safety Acceptable Use Rules - Letter to Parents/Carer for Primary or Secondary

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet, E-mail and personal on-line space.

In order to support the school in educating your child/young person about e-Safety (safe use of the Internet), please read the following Rules with your child/young person then sign and return the slip.

In the event of a breach of the Rules by any child or young person, the e-Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child/young person about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact the Headteacher.

Yours faithfully,

.....

e-Safety Acceptable Use Rules Return Slip, 200x – 200x

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

Key Stage 1 Rules

These are my rules for using the Internet safely.

My Internet and E-mail Rules

- I learn how to use the Internet.
- I use the Internet safely to help me learn.
- I can write polite and friendly e-mails or messages to people that I know.
- I can send and open messages with an adult.
- I only tell people my first name.
- I learn to keep my password a secret.
- I know who to ask for help.
- If I see something I do not like I know what to do.
- I know that it is important to follow the rules.
- I am able to look after others by using the Internet safely.
- I can go to www.thinkuknow.co.uk for help.

Key Stage 2 Rules
These are my rules for using the Internet safely and responsibly.

My On-line Rules
• I use the Internet to help me learn and I will learn how to use the Internet safely and responsibly. • I will send e-mails and messages that are polite and friendly. • I will only e-mail, chat to or video-conference people an adult has approved. • I will ensure that adults are aware when I use on-line communication tools, such as video-conferencing. • I will never give out passwords or personal information (like my surname, address or phone number). • I will never post photographs or video clips without permission and will never include names with photographs. • If I need help I know who to ask. • If I see anything on the Internet or in an e-mail that makes me uncomfortable, I know what to do. • If I receive a message sent by someone I don't know I know what to do. • I know I should follow the rules as part of the agreement with my parent/carer. • I am able to look after others by using the Internet in a safe and responsible way. • We know that I can go to www.thinkuknow.co.uk for help.

Key Stage 3 and 4 Rules

Secondary e- Safety awareness for students

I am encouraged to use and be aware of the safety rules and procedures which regulate my use of the ICT resources, including INTERNET. At XXXXX, I am encouraged and allowed to access the curriculum network and the Internet, enabling me to use vast resources and communicate, in support of research and education.
I will use these facilities for educational purposes and in an appropriate manner. I am responsible for my behaviour and communication. I know that any breach of the rules will be considered a disciplinary matter.

- I know access to the networked resources is a privilege. I am encouraged to make use of the Internet in support of my studies in all subjects.
- I need to make sure I am supervised when I use the Internet at school or at home.
- I will not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to myself and others.
- I will follow my teacher's instructions carefully.
- I must have permission from my parents/carers before I can use the Internet for my own independent research at school.
- I will endeavour to work with a friend when I am browsing the Web and ask "Is it true?" I do not assume that information published on the Web or written in an e-mail is accurate or true.
- I will keep my username and password private and will not tell anyone what they are.
- When I use e-mail, I will only write to 'net pals' or mentors approved by my teacher in school.
- I will be careful about what I write. I will check my work before I print or send anything. I will not use bad language. I will not write racist, sexist, abusive, homophobic or aggressive words. I will not write things that could upset and offend others as I could give myself and the school a bad name.
- I will not ever give personal information about myself or anyone else, such as our address, telephone number and private details in an e-mail or on a Website. I know I could put myself or others in danger.
- I will not respond to bad e-mail messages. I will let my teachers know immediately if I am sent anything I do not feel comfortable with.
- I will be a wise net surfer. I will not go to sites or download any materials, which are offensive, violent and pornographic.
- I will always respect the privacy of other users' files.
- I will report any incident that breaches the Acceptable Use Policy rules immediately to my teacher.
- I know that I can go to www.thinkuknow.co.uk for help.

Guidance: What do we do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: **webalerts@synetrix.com**).
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.

3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-safety officer.

The school may wish to consider delivering a parent workshop for the school community

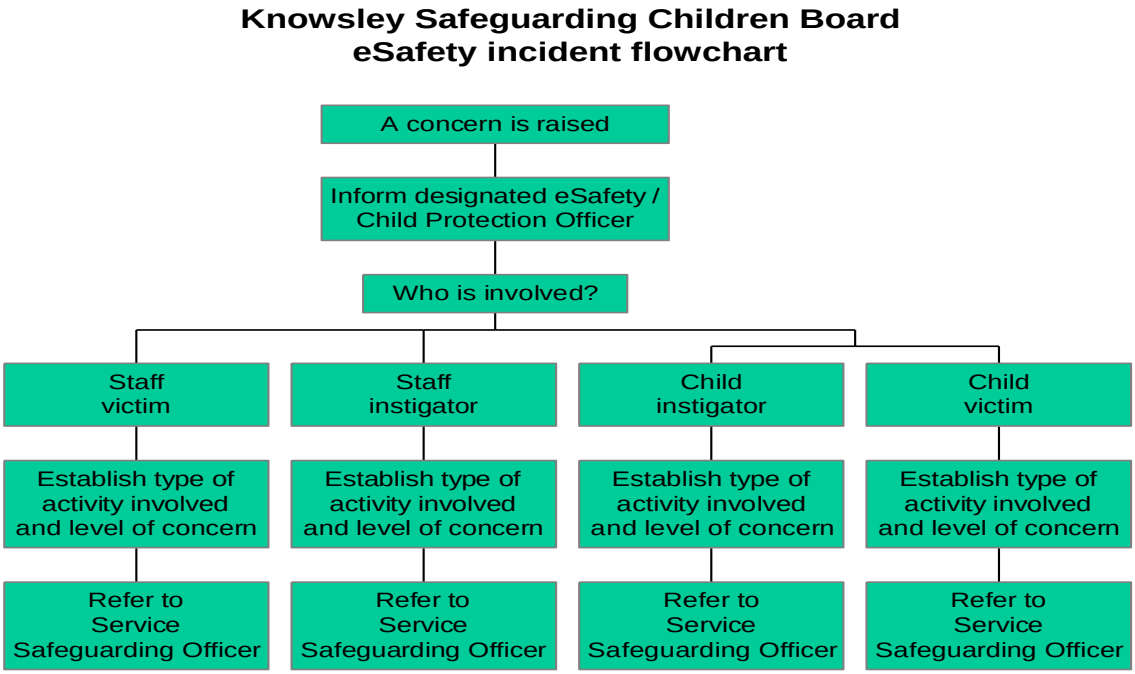
You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA e-safety officer.
6. Consider delivering a parent workshop for the school .community.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Reporting an Incident Workflow Diagram



Further Information and Guidance

The nature of e-safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

Internal documents

- KSCB Inter agency safeguarding Children Procedures
- Child Protection Policy
- Home School Agreement
- Social Networking Guidance http://knowit.kmbc/Resources/Document Library/Social networking guidance.doc
- Data Security http://knowit.kmbc/Resources/Document Library/Data Security Guidance.doc
- ICT Policy http://knowit.kmbc/C15/Policies and Procedures/Document Library/Policies and Procedures/section 3 employment practices/3.16 - ICT Policy for Employees.doc
- Data Protection http://knowit.kmbc/C5/Freedom%20of%20Information/default.aspx
- Data Security Guidance http://knowit.kmbc/Resources/Document Library/Data Security Guidance.doc
- Officers Code of Conduct http://knowit.kmbc/C18/C18/Human Resources/Document Library/Policies and procedures/Section 3 Employment practices/3.9.doc

External information

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk – (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)
- www.becta.org.uk (advice for settings to update policies) and http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)

- http://www.Knowsley.gov.uk/NACPC/acpc_home.htm (Local Safeguarding Children's Board Knowsley – policies, procedures and practices, including Section 12 of the Allegations Procedures are available here)

- www.nen.gov.uk/esafety (for schools and settings – access to the National Education Network)

- https://northants.lpplus.net (for schools and settings to access the Northants Learning Platform – click on the e-Safety tab for up-to-date information)

www.childnet-int.org (for a range of materials to support e-s