E- Safety Policy

for

Lawford C of E Primary School

Approved by Standards Committee on: June 27th 2013
Approved by Full Governing Body on: July 3rd 2013

Updated September 2017
Changes to be approved at the Standards and Safeguarding meeting on November 1st 2017
Introduction

Background and rationale

Development, monitoring and review of the Policy

Schedule for development, monitoring and review

Scope of the Policy

**Roles and Responsibilities**
- Governors
- Headteacher and Senior Leaders
- E-Safety Officer
- ICT Technician
- Teaching and Support Staff
- Designated Person for Child Protection
- E-Safety Committee
- Pupils
- Parents / Carers

**Policy Statements**
- Education – Pupils
- Education – Parents / Carers
- Education – Extended Schools
- Education and training – Staff
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Curriculum
- Use of digital and video images
- Data protection
- Communications
- Unsuitable / inappropriate activities

**Appendices:**
- Pupil Acceptable Use Policy Agreement
- Staff and Volunteers Acceptable Use Policy Agreement
Introduction

The Lawford C of E Primary School e-Safety Policy considers all current and relevant issues, in a whole school context, linking with our other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies.

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its “Safeguarding Children in a Digital World” suggested:

“That schools support parents in understanding the issues and risks associated with children’s use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too.”

The Byron Review “Safer Children in a Digital World” stressed the role of schools:

“One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children’s workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area.”

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to “outweigh the risks.” However, we must, through our e-safety policy, ensure that we meet our statutory obligations to ensure that our children are safe and are protected from potential harm, both within and outside school. This policy will also form part our school’s protection from legal challenge, relating to the use of ICT.
This policy reflects the view that safe internet access is an entitlement for all learners.

An effective School e-Safety Policy is owned and accepted by the whole school community.

Consultation in the production of this policy will involve:

• Governors, Teaching Staff and Support Staff, Pupils and Parents

Background and Rationale

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child’s education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. The ‘Keeping Children Safe in Education’ document (updated September 2016) has advice about online safety in Annex C (page 62) which should be read in conjunction with this policy.

‘Schools must ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. It is also important that schools teach pupils about online safety more generally.’

Some of the other dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual’s consent or knowledge
• Inappropriate communication / contact with others, including strangers
• Cyber-bullying
• Access to unsuitable video / internet games
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help our children (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

**Development, Monitoring & Review of this Policy**

**This e-safety policy is being developed through consultation with:**

• School E-Safety Officer
• Head teacher
• Teachers
• Support Staff
• ICT Technical staff
• Governors
• Parents and Carers

**Consultation with the whole school community will take place through the following:**

• Staff meetings
• School Council
• Governor committee meeting
• School website and newsletters
## Schedule for Development, Monitoring and Review

<table>
<thead>
<tr>
<th>Description</th>
<th>Dates/Persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>This e-safety policy was approved by the Governors’ Sub Committee on:</td>
<td>June 27th 2013</td>
</tr>
<tr>
<td>Full Governing Body on:</td>
<td>July 3rd 2013</td>
</tr>
<tr>
<td>The implementation of this e-safety policy will be monitored by:</td>
<td>E-Safety Officer</td>
</tr>
<tr>
<td>The Senior Leadership Team</td>
<td>E-Safety Officer</td>
</tr>
<tr>
<td>Monitoring will take place at regular intervals:</td>
<td>Once a year</td>
</tr>
<tr>
<td>The Governing Body will receive a report on the implementation of the</td>
<td>Summer Full Governing Body Meeting</td>
</tr>
<tr>
<td>e-safety policy generated by the monitoring group (which will include</td>
<td></td>
</tr>
<tr>
<td>anonymous details of e-safety incidents) at regular intervals:</td>
<td></td>
</tr>
<tr>
<td>The E-Safety Policy will be reviewed annually, or more regularly in the</td>
<td>Autumn 2018</td>
</tr>
<tr>
<td>light of any significant new developments in the use of the technologies, new threats to</td>
<td></td>
</tr>
<tr>
<td>e-safety or incidents that have taken place. The next anticipated review</td>
<td></td>
</tr>
<tr>
<td>date will be:</td>
<td></td>
</tr>
<tr>
<td>Should serious e-safety incidents take place, the following external</td>
<td>LA ICT Manager, LA Safeguarding Officer, Police Commissioner’s Office</td>
</tr>
<tr>
<td>persons / agencies should be informed:</td>
<td></td>
</tr>
</tbody>
</table>

**The school will monitor the impact of the policy using:**

1. Logs of reported incidents
2. Surveys / questionnaires of
   - Pupils (e.g. Ofsted “Tell-us” survey / CEOP ThinkUknow survey)
     [www.thinkuknow.co.uk/8_10/Survey/](http://www.thinkuknow.co.uk/8_10/Survey/)
   - Parents / carers responding to questionnaires at E-Safety evenings held in the school.
Scope of the Policy
This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities
The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

• regular meetings with the E-Safety Officer
• regular monitoring of e-safety incident logs
• reporting to relevant Governors committee meeting

Head teacher and Senior Leaders:

• The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.

• The Head teacher / Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

• The Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

• The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer. The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
E-Safety Officer:

- leads on e-safety and liaises with ICT/e-safety linked governor
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

ICT Technician:

The ICT Technician is responsible for ensuring:
- that the school has an effective anti-virus programme in place
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy
- that school is keeping up to date with e-safety information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that monitoring software and systems are implemented and updated as agreed in school policies

Teaching & Support Staff:

Teaching and support staff are responsible for ensuring that:
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Officer and Head teacher for investigation
- digital communications with pupils (email) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they monitor ICT activity in lessons, extra curricular and extended school activities
• they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
• in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer
should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
• sharing of personal data
• access to illegal / inappropriate materials
• inappropriate on-line contact with adults / strangers
• potential or actual incidents of grooming
• cyber-bullying

Pupils:
• are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. At KS1 parents / carers sign on behalf of the pupils.
• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• where appropriate, will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school.
• Pupils that have access to email from the 'lawford.essex.sch.uk' domain have a default setting that only enables them to email within that domain and not email externally.
Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through annual e-safety parents’ evenings, newsletters, letters, website and information about national or local e-safety campaigns and literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school’s e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT and PHSE lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities, visits from police officers informing children about the dangers online and through discussion and assemblies.
- KS2 pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the student pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils are be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems and the internet will be posted in all classrooms.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.
- Pupils made aware of cyberbullying and that any accusations or reports will be taken seriously in line with the school’s anti-bullying policy.
Education – parents and carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:
- Letters, newsletters, web site
- E-safety parents evening with local police officer or other appropriately trained persons.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- A planned annual event of e-safety training will be made available to staff. The e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Officer will provide advice and guidance to individuals as required.
- Staff are reminded about e-safety protocols within the safeguarding training during the non-pupil days at the start of each academic year. E-safety notices and updates, where applicable, are part of the weekly briefing for all staff. More formal training is delivered as part of an e-safety evening for parents, which staff are expected to attend and governors are invited to.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
The Prevent Duty June 2015 page 10 states that:

IT policies

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school’s ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website.

It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets this Policy and guidance
- There will be regular reviews of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located
- All users will have clearly defined access rights to school ICT systems.
- Pupils may use class or group log-ons to access the network, where appropriate, e.g. assembly crew
- All users will be provided with a username and staff access will be through a password. Users will be required to change their password on a regular basis.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe and Head teacher’s locked file)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers visitors) onto the shared school access folder. (a.teacher)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit and ensure that Google Safesearch is being used.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Lawford C of E Primary School Child Protection Policy (updated July 2017) states:

‘Peer on peer abuse can manifest itself in many ways. This may include bullying (including cyber bullying), on-line abuse, gender-based abuse, ‘sexting’ or sexually harmful behaviour. We do not tolerate any harmful behaviour in school and will take swift action to intervene where this occurs.’

Prevention of radicalisation

As of July 2015, the Counter-Terrorism and Security Act (HMG, 2015) placed a new duty on schools and other education providers. Under section 26 of the Act, schools are required, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”. This duty is known as the Prevent duty.

It requires schools to:

- teach a broad and balanced curriculum which promotes spiritual, moral, cultural, mental and physical development of pupils and prepares them for the opportunities, responsibilities and experiences of life and must promote community cohesion.
- be safe spaces in which children / young people can understand and discuss sensitive topics, including terrorism and the extremist ideas that are part of terrorist ideology, and learn how to challenge these ideas.
- be mindful of their existing duties to forbid political indoctrination and secure a balanced presentation of political issues.
Our school works in accordance with the PREVENT Duty and approaches this issue in the same way as any other child protection matter. Any concerns that one of our pupils is at risk in this respect, will be referred to Children’s Social Care in line with the SET procedures.

CHANNEL is a national programme which focuses on providing support at an early stage to people identified as vulnerable to being drawn into terrorism. Our staff understand how to identify those who may benefit from this support and how to make a referral.

**Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet.

Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils and staff must not take, use, share, publish or distribute images of others in school without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- **Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.**
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website as part of the agreement signed by parents when a child joins the school
Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate
• Kept no longer than is necessary
• Processed in accordance with the data subject’s rights
• Secure
• Only transferred to others with adequate protection.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
• Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
• Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

• **the data must be encrypted and password protected**
• the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
• the device must offer approved virus and malware checking software
• the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

<table>
<thead>
<tr>
<th>Communication Technologies</th>
<th>Staff &amp; other adults</th>
<th>Pupils</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile phones may be brought to school</td>
<td>Allowed</td>
<td>x</td>
</tr>
<tr>
<td>Use of mobile phones in lessons</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of mobile phones in social time</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Taking photos on mobile phones</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of personal email addresses in school, or on school network</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of school email for personal emails</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of chat rooms / facilities</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of instant messaging</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use of social networking sites</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses or public chat / social networking programmes must not be used for these communications.
- Upper KS2 will be provided with individual school email addresses for educational use.
• Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**Unsuitable and inappropriate activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
This Acceptable Use Policy is intended to ensure:

- that our children will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that children will have good access to ICT to enhance their learning and will, in return, expect our children to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person’s username and password.
- I will be aware of “stranger danger”, when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I will act as I expect others to act toward me:
- I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others
- I will not take or distribute images of anyone without their permission.

I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). Please complete the sections on
the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:
• I use the school ICT systems and equipment (both in and out of school)
• I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name of Pupil

Class

Signed ___________________________ Date ___________________________
Staff (and Volunteer) Acceptable Use Policy Agreement

Lawford C of E Primary School Policy

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
• that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
• I understand that the school will monitor my use of the ICT systems, email and other digital communications.
• I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school.
• I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
• I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password.
• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
I will be professional in my communications and actions when using school ICT systems:

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g., on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials, which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential,
except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action, a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date