Our Lady of Muswell Catholic
Primary School

One community
Love of Learning
Making time for God

E safety Policy

Date for Review: January 2020

Contents

Introduction

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, it is recommended 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, furthermore schools should 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 and young people 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. At OLM we 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.”

At OLM, our aim is to ensure that our children are safe and are protected from potential harm, both within and outside school. We believe that safe internet access is an entitlement for all learners

Due to the ever changing nature of Information and Communication Technologies, it is best practice that the school reviews the E-Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Background/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 and young people should have an entitlement to safe internet access at all times.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the 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 (sexting, sextortion)
- 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.

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.

Schedule for Development/Monitoring/Review

The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator / Senior Leadership Team/ E safety Governor
Monitoring will take place at regular intervals:	At least once a year
The Governing Body will receive a report on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at regular intervals:	At least once a year as part of HT report
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.	Spring Term following Safer Internet Day
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	E safety Governor, Safeguarding Governor, SIA, LA Safeguarding Officer

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Pupil Voice
- Feedback from parents
- Feedback from staff

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 Headteachers, 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 reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety. The role of the E-Safety Governor will include regular updates from the E-Safety Co-ordinator, The safeguarding governor will monitor e-safety incident logs. reporting to FGB.

Headteacher and Senior Leaders:

- The Headteacher 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 Co-ordinator
- The Headteacher / 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 will receive regular monitoring reports from the E-Safety Officer.
- The Headteacher and the deputy Head Teacher 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. (see COLFS flow chart on dealing with e-safety incidents included in a later section – “Responding to incidents of misuse” and relevant disciplinary procedures)

E-Safety Co-ordinator:

- 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. Any investigation/action/sanctions will be the responsibility of the Head Teacher or Deputy Head Teacher
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- updates the E-Safety Governor to relay current issues

- review incident logs and report regularly to Senior Leadership Team

Data Protection Officer (DPO)

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ and ‘Data protection: a toolkit for schools’ (April 2018), especially this quote from the latter document:
    - GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding
- The same document states that the retention schedule for safeguarding records may be required to be set as ‘Very long term need (until pupil is aged 25 or older)’
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Technical staff:

The ICT Technician is responsible for ensuring:

- that the school’s ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance(LGFL)
- that users may only access the school’s networks through a properly enforced password protection policy, in which passwords are regularly changed
- that he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

Teaching and 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 / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Officer/Headteacher
- digital communications with 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, extracurricular 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.

- 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

Designated person for child protection:

The designated person for child protection should be trained in e-safety 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
- 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
- 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 E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/carers:

Parents/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. We will attempt to take every opportunity to help parents understand these issues e.g. through parents' evenings, newsletters, letters, signposting literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy

Community Users:

Any Community Users who access school ICT systems as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

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. We aim to support our children in recognising and avoiding e-safety risks and build their resilience.

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

- E-safety is delivered as part of the ICT curriculum and are regularly revisited
- The national annual safer internet day is used as a focus to impart key e-safety messages
- 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 helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should 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 / internet will be displayed in all rooms
- Staff should act as good role models in their use of ICT and the internet and any mobile devices

Education–parents/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 / 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).

OLM are committed to supporting parents and carers.

Education and 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 programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme and fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Co-ordinator will receive regular updates of current practice
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Co-ordinator will provide advice/guidance/training as required to individuals

Training-Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any group involved in ICT/e-safety/health and safety/ child protection.

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. 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

- There will be regular reviews and audits of the safety and security of school ICT systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems**.**
- All users will be provided with a username and password by the ICT technician who will keep an up to date record of users and their usernames. Users will be required to change their password annually.
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure
- 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.
- The school maintains and supports a managed filtering service provided by LgfL
- Any filtering issues should be reported immediately to the E-safety co-ordinator.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head Teacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Officer
- *A*greed procedures are in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- Only the ICT technician has permissions to install programmes on school workstations / portable devices.
- 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.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Requests should be made to the Head Teacher
- 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.

Use of digital and video images

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 must not take, use, share, publish or distribute images of others 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 should 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
- Pupil's work can only be published with the permission of the pupil and parents or carers.

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**.**

GDPR

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, **appropriate organisational and technical safeguards should still be in place […]** Remember, **the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding**."

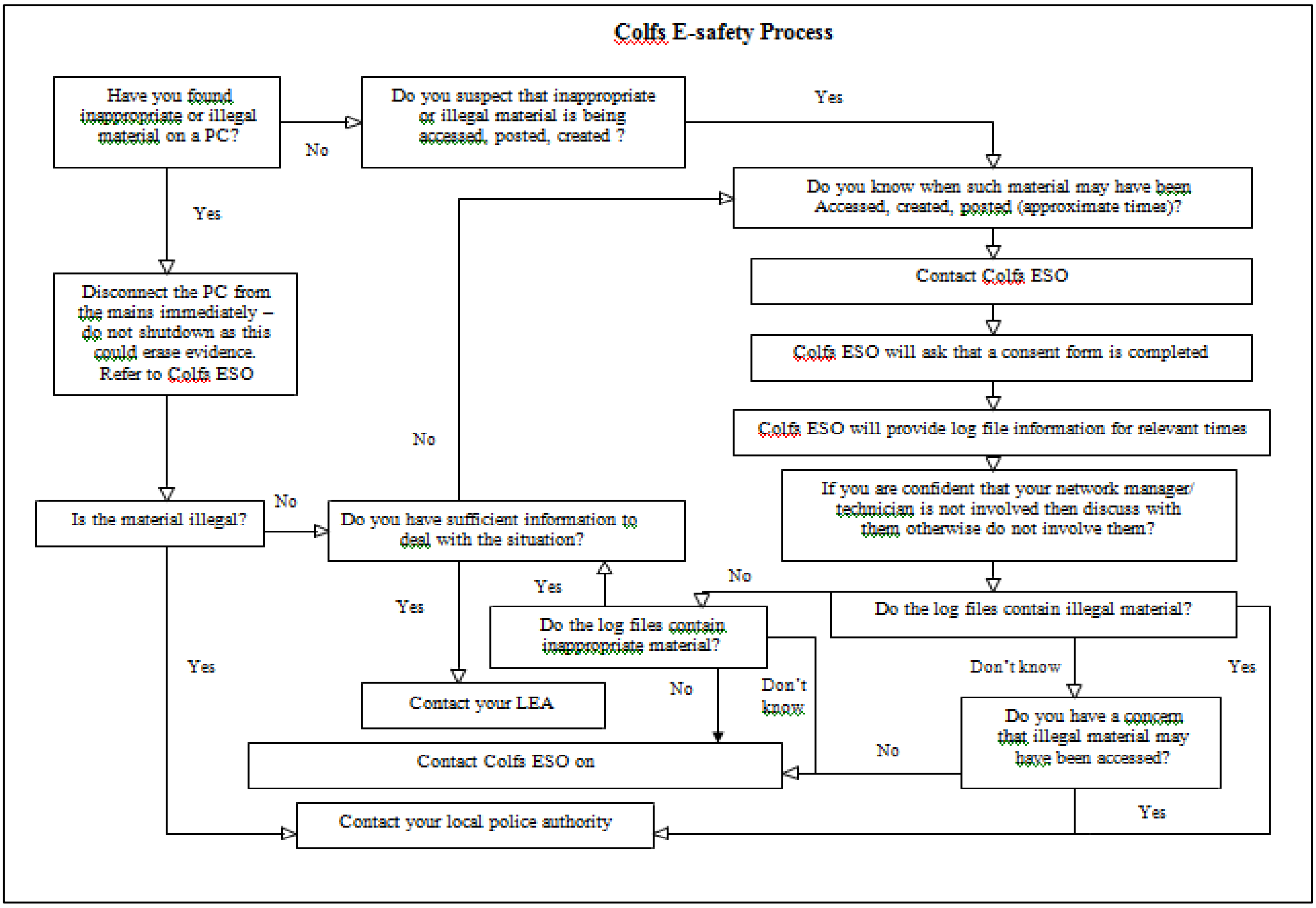
All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy.

Rigorous controls on the LGfL TRUSTnet network, USO sign-on for technical services, firewalls and filtering all support data protection. The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.
Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If any apparent or actual misuse appears to involve illegal activity (i.e. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material, other criminal conduct, activity or materials), the flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.


Colfs E-safety Process
Have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed, posted, created ?
Yes
Do you know when such material may have been Accessed, created, posted (approximate times)?
Yes
Contact Colfs ESO
Colfs ESO will ask that a consent form is completed
Colfs ESO will provide log file information for relevant times
Disconnect the PC from the mains immediately – do not shutdown as this could erase evidence. Refer to Colfs ESO
No
If you are confident that your network manager/ technician is not involved then discuss with them otherwise do not involve them?
Is the material illegal?
No
Do you have sufficient information to deal with the situation?
Yes
No
Do the log files contain illegal material?
Yes
Yes
Do the log files contain inappropriate material?
Yes
Don't know
Yes
Contact your LEA
No
Don't know
Do you have a concern that illegal material may have been accessed?
No
Contact Colfs ESO on
Yes
Contact your local police authority

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/ disciplinary procedures.

Pupil Acceptable Use Policy Agreement – KS1 / Foundation

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. Young people should have an entitlement to safe internet access at all times.

KS1 / Foundation

These rules will be shared with the children by the staff who work in Key Stage 1. Children will be reminded of them when required. Rules will be on display by the computers so all staff/volunteers are aware of what the children are allowed to do and what rules to reinforce.

- I will ask an adult if I want to use the computer.
- I will always keep my passwords a secret. I will not tell people about myself online (My name, family information, journey to school, my pets and hobbies are all examples of personal details). I will not give my mobile phone number to anybody who is not a friend in real life.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or my parents if I see anything that makes me uncomfortable or scared when online.
- I will tell an adult if I see someone else breaking the rules.
- I know that adults can check what I have been doing on the computer.
- I will make sure all messages or comments are polite.
- I will tell a teacher or my parents if I receive a nasty message or get sent anything that makes me uncomfortable when online. I will not reply to any nasty message.
- I will never agree to meet a stranger. I will not load photographs of myself onto a computer.
- I know that if I break these rules, I might not be allowed to use a computer.

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
- 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,

Name of Pupil

Class

Signed Date

Pupil Acceptable Use Policy Agreement – KS2

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. Young people should have an entitlement to safe internet access at all times.

KS2

These rules will be shared with the children by the staff who work in Key Stage 2. Children will be reminded of them when required. Rules will be on display by the computers so all staff/volunteers are aware of what the children are allowed to do and what rules to reinforce.

- I will only use my own username and password.
- I will always keep my passwords a secret.
- I will always keep my personal details private (My name, family information, journey to school, my pets and hobbies are all examples of personal details).
- I will not try to get past any security measures in place to protect the school network.
- I will only visit sites that are appropriate to my work at the time.
- I will tell a responsible adult if I see anything that makes me scared or uncomfortable when online.
- I will make sure all emails I send are respectful.
- I will make sure all messages or comments I send are respectful.
- I will tell a responsible adult if I receive a nasty message or get sent anything that makes me uncomfortable when online.
- I will not reply to any nasty message or anything that makes me feel uncomfortable.
- I will only email or message people I know or those approved by a responsible adult.
- I will talk to a responsible adult before joining chat rooms or networking sites.
- I will never meet an online friend without taking a responsible adult that I know with me.
- I will always check with a responsible adult before I show photographs of myself.
- I will use ICT equipment safely and responsibly.
- I will only use school ICT equipment for my work.
- I will not give my mobile phone number to anyone who is not a friend.
- I will always check with a responsible adult before I show photographs of myself.

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
- 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,

Name of Pupil

Class

Signed Date

Acceptable usage agreement staff

New technologies have become integral to the lives of children and young people in today's society, both within school 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 staff

I understand that I must use school ICT systems in a responsible way, to ensure that there

- 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 OLM ICT systems (e.g. laptops, email) out of OLM
- I understand that the schools 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 not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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's in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school emails. Any such communication will be professional in tone and manner.
- I will not engage in any on-line 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 (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 use personal email addresses on the school ICT systems.
- 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.
- 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
- 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 Data 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. This could include 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

Parental acknowledgement

Name of Pupil

Class

As the parent / carer of the above, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will continue to receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the AcceptableUse Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed Date