St Francis Xavier
Catholic Primary School

JESUS HOLDS US IN THE PALM OF HIS HAND

E-Safety Policy

Created by
ICT Co-ordinator

1. Introduction to E-safety

E-safety is the school's ability to protect and educate pupils and staff in their use of technology and to have appropriate mechanisms to intervene and support any incident where appropriate. 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 E-Safety Policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti –bullying policies. The development and implementation of this policy involved all the stakeholders in the school from the headteacher and governors to the senior management, classroom teachers, support staff, parents, members of the community and the pupils themselves.

Our school takes an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT also. ICT is one area where the pupils often have more skills and knowledge than their parents.

The Byron Review "Safer Children in a Digital World" clearly states that schools must take an active role in advising parents on keeping pupils safe on the internet at home. Our school will empower pupils and raise the skills of parents. E-safety is embedded in our new ICT curriculum (2012). In addition throughout the year we have regular updates as and when new technologies emerge and new resources become available.

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. Our school has made a significant investment both financially and physically to ensure these technologies are available to all learners. This e-safety policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

2. Why is e-safety important?

Technology offers unimaginable opportunities and is constantly evolving. There has been a proliferation of new technologies e.g. smartphones, ipads, notebooks, laptops, touchscreens, games consoles, ipod, WII, desktops etc. Younger and younger pupils are becoming skilled in these technologies but these skills also bring new risks. These risks have to be identified and managed within and outside school.

91% of children live in a household with access to the internet through a PC, laptop or netbook
9% of 3-4s use a tablet, **6%** of them using a tablet to access the internet at home.
37% of 3-4s use the internet through a PC, laptop or netbook at home
4% of 3-4s use the internet at nursery
14% of children aged 5-7 and **24%** aged 8-11 use the internet alone.
14% of all children aged 5-15 use a tablet computer (such as an iPad) at home.
22% of children aged 8-11s say they have a social networking profile and have an average of 92 friends and have never met **12%** of them.
4% of children aged 8-11s have been bullied online
30% of children aged 8-12 who use the internet at home say they have a profile on Facebook, Bebo or MySpace even though there is a minimum age restriction (age13). **99%** of these children have a Facebook profile.
One in three boys who play games online do so against people not known to them.

Ofcoms Children and parents: media use and attitudes report 2012 (23/10/12)

3. The Risks

The risks can be classified into three main areas:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images)
- copyright (little care or consideration for intellectual property and ownership (for example music and film))

Ofsted Inspecting e-safety September 2012

Some of the risks reflect situations in the off-line world; therefore our 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 the 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 young people (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.

4. The Development/Review and Monitoring of this Policy

This e-safety policy has been developed by the ICT Co-ordinator, However, it is a working document and contributions of all stakeholders are included which are made up of governors, senior management, staff, support staff, external technician support (Innovit) and the pupils themselves as they identify emergent risks.

- *Mrs M Simmons- Headteacher and School Safety Officer*
- *Senior Management*
- *ICT co-ordinator- Carole Rush*
- *Teachers*
- *Support Staff*
- *External ICT Technical staff (Innovit)*
- *Governors*
- *Parents and Carers*
- *Community users*

Consultation with the whole school community has taken place through the following:

- *Weekly meetings (ICT co-ordinator with the ICT technician Service Level Provider).*
- *CPD Meetings on e-safety*
- *Staff meetings*
- *Governors meetings*
- *School Pupil Council meetings*
- *School website*
- *Teacher ICT Survey and feedback*
- *Parent ICT Survey and feedback*
- *Pupil ICT Survey and feedback*

5. Schedule for the Development/Review and Monitoring of this Policy

This e-safety policy was approved by the **Governing Body on:**	*Date to be agreed*
The implementation of this e-safety policy will be monitored by the:	*ICT co-ordinator* *Mr A Dickinson* *Innovit*
Monitoring will take place at regular intervals:	*Termly* *Embedded throughout the whole school in the ICT curriculum* *ICT Internet Safety Day (5th February 2013)*
The **Governing Body** will receive a report on the implementation of the e-safety policy generated by ICT co-ordinator which will include details of e-safety incidents	*The report will be attached to the revised e-safety policy (November 2013)*
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. The next anticipated review date will be:	*Annual review* *or* *as and when new emergent risks are identified*
Should **serious** e-safety incidents take place, the following external persons / agencies should be informed:	*The local police* *CEOP* *Childline 0800 1111* *Local Authority Safety officer or e-safety service level provider*

How the School Monitors the Impact of the e-safety Policy

- Logs of reported incidents in the Class Incident Behaviour Books
- E-safety evidence in Subject Leader Folder
- Reply slips of parent feedback in Subject Leader Folder
- Surveys / questionnaires in Subject Leader Folder
  - pupils
  - parents / carers
  - staff

NB: The school has strong internet filters provided by Broadband Sandwell. There has been NO internet exposure to inappropriate content reported within school to date. The cost of this service has risen significantly, however the benefits and the safeguarding of our pupils far outweighs the additional costs involved in retaining this service.

From April 2013 e-safety training and provision will be provided by Broadband Sandwell

6. Scope of the Policy

This policy applies to all members of the school community (including staff, students, 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 2011 includes the following:

Key points of the Education and Inspections Act 2011

- Teachers have statutory authority to discipline pupils for misbehaviour which occurs in school and, in some circumstances, outside of school. **(This includes the use of ICT).**
- The power to discipline also applies to all paid staff (unless the head teacher says otherwise) with responsibility for pupils, such as teaching assistants. **(This includes the use of ICT).**
- Heads and governing bodies must ensure they have a strong behaviour policy to support staff in managing behaviour, including the use of rewards and sanctions. **(This includes the use of ICT).**
- Governing bodies have a duty under section 175 of the Education Act 2002 requiring them to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children. **(This includes the use of ICT).**

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

7. 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 receiving regular information about e-safety incidents and monitoring reports. The headteacher has:

- regular meetings with the E-Safety Co-ordinator
- regular meetings with the Senior Management
- regular monitoring of e-safety incidents (to be recorded in classroom Incident Books)
- reporting to Governors committee

Headteacher and Senior Management:

- 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 has ensured that that the E-Safety Coordinator / 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 Headteacher and the Senior Management Team 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 Headteacher and the Senior Management 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 Coordinator / ICT co-ordinator

- leads the e-safety within and outside school
- 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 e-safety authority (Broadband Sandwell)
- liaises with ICT technical staff (external)
- receives reports of e-safety incidents which are recorded in the Classroom Incident Books
- meets regularly with the headteacher to discuss current issues, review incident logs and filtering • attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Technician Support (Innovit)/ (Network Manager)

Innovit (ICT Service Provider) takes the role of the Network Manager and 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 the School's Internet Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that the technician's e-safety technical information is up to date in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (Openhive) / remote access / email is regularly monitored in order that any misuse (Openhive) / attempted misuse can be reported to the E-Safety / ICT Co-ordinator /Headteacher / Class teacher / support staff for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies and not compromised

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 ICT Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety/ICT Co-ordinator / Headteacher / Senior Management / Class teacher / for investigation / action / sanction

- digital communications with students / pupils (email / Virtual Learning Environment (Openhive) / voice) should be on a professional level and staff should only use official school systems e-mail
- 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 and implement current school policies with regard to these devices. Staff mobile phones should be placed in lockers during school hours.
- in lessons where internet use is pre-planned students / pupils should be taught how to search correctly in order to reduce the risk of exposure to inappropriate content

Child Protection Officer/Headteacher

The Officer should be aware of 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. Parents of pupils in Nursery, Reception, Year 1 and Year 2 will 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 and illegal materials and know how to do so.
- will be expected to know and understand school policies on the use of digital cameras and hand held devices. Pupils are not allowed to use mobile phones in school. 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.

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. The school will therefore take every opportunity to help parents understand these issues through letters home, school website, Openhive and local e-safety campaigns. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website and Virtual Learning Environment (Openhive).
- returning reply slips for pupils watching the Think You Know resources that are age appropriate for their children www.thinkuknow.co.uk

Community Users

Community Users who access school ICT network systems will be expected to sign a Community User AUP before being provided with access to school systems.

8. 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 and young people 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 will be provided by the ICT co-ordinator using the Think you know resources and will be tailored to individual age groups. Evidence will be placed in the Subject Leader Folder.
- Key e-safety messages are reinforced as part of a planned programme during Internet Safety Day across the whole school.
- 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.
- E-safety is embedded in the ICT curriculum using the Rising Stars Switch on ICT Schemes of Work.
- 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
- E-safety rules are displayed in the ICT Suite and around the school
- Staff should act as good role models in their use of ICT, the internet and 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).
The school will therefore seek to provide information and awareness to parents and carers through

- Letters giving links to the Thinkuknow website and asking parents to watch the resources with children (the letter contains a reply slip)
- Providing a parent page on Openhive enabling them to access e-safety resources
- Providing parents with links to free monitoring software which keeps pupils safe on line (Norton Family Online)

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 programme of formal e-safety training will be made available to staff. An audit of 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 Coordinator will receive regular updates through attendance at ICT co-ordinators CPD courses
- The E-Safety Coordinator will receive regular updates through attendance at ICT co-ordinators school hub meetings.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Training – Governors

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

- Participation in school training / information sessions for staff or parents

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.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the School Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy guidance
- 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 as defined in the Security Policy.
- All pupils currently have yearly group logins to the school network.
- All pupils from Y1-Y6 have individual e-mail addresses
- All teachers and support staff have individual logins and e-mail addresses
- All short term students have guest logins (less than 6 weeks)
- All trainee teacher long term students (6 weeks and longer) have individual logins and e-mail addresses with teacher access rights
- The master administrator password is made available to the Headteacher and kept in a secure place (safe)
- There must always be 2 active administrator passwords at all times
- The administrator password in not available to the ICT co-ordinator therefore the co-ordinator cannot be held accountable and responsible for any actions carried out by the external support contractor.
- Monitoring of the contractors actions must be carried out by the Senior Management Team who do have access to the Administrator Password. An administrator password has been made available to Mr Dickinson – Deputy Headteacher
- Users will be made responsible for the security of their username and password and they 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.
- Support staff will have teacher access rights.
- Requests from staff for sites to be removed from the filtered list must be approved by Senior Management
- Appropriate security measures provided by Innovit (external contractors) 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.
- All staff except the ICT co-ordinator, Senior Management and Administrator (Innovit) are forbidden from downloading executable files
- All teacher laptops must have fingerprint encryption setup
- All teaching staff have been provided with an encrypted memory stick
- 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
-

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: data must be encrypted and password protected
- the device must be scanned by the antivirus and malware checking software as soon as it is inserted into the system
- the data must be securely deleted from the device once it has been transferred or its use is complete

Communications

The school may also wish to add some policy statements about the use of communications technologies, in place of, or in addition to the above 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 (Openhive)
- The receipt of any email that makes people feel uncomfortable, suspicious, is offensive, threatening or bullying in nature and must not be responded to and should be reported to the ICT co-ordinator.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- All pupils have Individual e-mail addresses from Year 1-6
- All staff and support staff have Individual e-mail addresses

Use of digital and video images

- Images of children to only be taken on school cameras (video and cameras)
- School cameras should not be taken off site except for educational purposes and visits.
- SD cards from cameras should not be taken out of the camera when loaned to other classes; this reduces the risk of becoming lost.
- School cameras should not be taken off site except for educational purposes (images deleted from SD cards can easily be restored)
- Images of children to be transferred onto the school network by the next working day wherever possible
- Images need to be stored securely on devices that will not be removed from the school, as it is important to note that any images downloaded onto laptops and then deleted can be restored.

The SMART Acronym

- Every pupil has been given the SMART rules which will be kept in school. Teachers must ensure that all pupils know the meaning of each letter

Responding to Incidents that are illegal

It is hoped that all stakeholders of the school and community will be responsible users of ICT, and that they 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**. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If the misuse involves illegal activity

- child sexual abuse images (even unintentional images that have slipped through the internet filters)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material and threats
- severe harassment and cyber bullying-it is possible that the perpetrators could be facing a criminal charge
- serious slander and defamation of someone’s character
- downloading programs, music, films and pictures that breaches copyright
- creating and propagating computer viruses

Procedures for dealing with illegal acts or illegal images

The advice from police about an illegal act

If an inappropriate image is found on a machine and this image may be illegal:
Never attempt an internal investigation, if illegal images or content are reported to the Head Teacher, the police should always be involved, only the police need to see the evidence. The police will clarify if the image is illegal or objectionable (hard core adult pornography falls into this objectionable category, not acceptable in school but not illegal). Objectionable should be dealt with by the school by following behaviour policy and acceptable use agreements.

- If anything is suspected to be illegal (or that school is not sure about) is found on the computer or any mobile device immediately secure the device. **Do not turn it off**. Evacuate the room to stop any exposure of images to other pupils. If the images are on a desktop PC turn off the **monitor but do not touch the computer.** Inform the Headteacher who will call the police. The police will confirm if the image is illegal or just unacceptable.
- **Do not go back and view the material** as you could **contaminate** the evidence. Opening and viewing illegal images may come under the category of a criminal offence. You change the date and time on the document, thus destroying the evidence.
- **Do not copy the evidence** as you are creating a copy of an illegal image.

Procedures for dealing with inappropriate activates which are legal but unacceptable

- Attempting to access or accessing the school network, using another pupil's account
- Allowing others to access the school network by sharing usernames and passwords
- Writing down passwords
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
- Staff using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school, such as comments and inappropriate photos on social networking sites
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Actions which could compromise the staff member's professional standing

9. Acknowledgements

- Broadband Sandwell
- SWGfL E-Safety website (e-safety template)
- Ofcoms Children and parents: media use and attitudes report 2012 (23/10/12)
- Ofsted Inspecting e-safety September 2012
- Byron Review – Children and New Technology – "Safer Children in a Digital World"

To be reviewed annually

Pupil/Parent Acceptance User Policy Agreement (PPAUP)

This Acceptable Use Policy is intended to ensure:

- that young people 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 pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils 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 can 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 to my teacher or adult in charge.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not alter computer settings unless given explicit permission from the ICT co-ordinator.
- I will not use the school ICT systems for on-line gaming, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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 use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use my mobile phone during lesson times and if brought into school they must be kept in the office.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation that sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- 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 only not use chat and social networking sites during lesson times unless directed by a teacher and it is for educational purposes

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to sanctions from school in accordance with the Behaviour Policy or in the event of illegal activities involvement of the police .

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. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student / 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 eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil

Year Group

Pupil Signature

Date

Parent Signature

Date

Pupils from Nursery, Reception and Year 1 do not need a pupil signature but do need a parent signature

Staff/Students (Volunteers) User Policy Agreement (SSVAUP)

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 students / 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 (eg laptops, email, Openhive, social networks 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 out of school hours and 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 (eg on the school website / Openhive) 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 at home
- I will only communicate with students / pupils and parents / carers using official school systems. 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.
- I will ensure I enable fingerprint encryption on my school laptop if it is available.

The school has 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 (ipads / laptops / mobile phones / USB encrypted 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 if required.
- I will not use personal email addresses on the school ICT systems unless there is a problem with the school e-mail system.
- 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 only use encrypted memory sticks in school and will delete any confidential information immediately after transfer to the system.
- I understand that data protection policy requires that any staff or student / 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 to the ICT Technician through the School ICT Fault Reporting System and not to the ICT Co-ordinator.
- 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 disable or cause any damage to school equipment, or the equipment belonging to others.
- I will monitor pupils to ensure they do not disable or change settings to the school equipment.
- I will monitor pupils to ensure that they transfer photos and videos to the system and delete the images from the portable device. In addition I will ensure all equipment is fully charged before returning to its secure place.

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 with particular reference to social network sites.
- 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

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

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

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2011

Key points of the Education and Inspections Act 2011

- Teachers have statutory authority to discipline pupils for misbehaviour which occurs in school and, in some circumstances, outside of school. **(This includes the use of ICT).**

- The power to discipline also applies to all paid staff (unless the head teacher says otherwise) with responsibility for pupils, such as teaching assistants. **(This includes the use of ICT).**

- Heads and governing bodies must ensure they have a strong behaviour policy to support staff in managing behaviour, including the use of rewards and sanctions. **(This includes the use of ICT).**

- Governing bodies have a duty under section 175 of the Education Act 2002 requiring them to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children. **(This includes the use of ICT).**

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