E-Safety Policy

St Francis' Catholic Primary School

Ensuring for all an excellent child-centred education within a Christ-centred philosophy

Approved by FGB on:	Jan 2018
Committee Responsible:	Curriculum
Next review due by:	Jan 2019

Policy for E-Safety

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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.

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 requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

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
- 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.

Aims

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:

- **Provide a planned e-safety programme as part of ICT / PHSE / other lessons**
- **Teach pupils in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**
- **Help pupils to understand the need to sign up (annually) to the pupil Acceptable Use Policy and encourage them to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school**
- **Teach pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Staff to 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.

- **The school will seek to inform parents and carers about e-safety risks and issues**

Education & Training - Staff

- **All staff receives e-safety training and understands their responsibilities, as outlined in this policy**
- **Help staff to understand the need to sign up (annually) to the staff Acceptable Use Policy and encourage them to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school**

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.**

Use of Digital and Video Images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

- **The school will inform and educate users about the risks of using digital and video images and will implement policies to reduce the likelihood of the potential for harm**

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**

Data Protection

- **Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998**

Personal data will 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.**

Responding to incidents of misuse

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse.
The school will aim to:

- **Deal with all incidents as soon as possible in a proportionate manner**
- **Deal with all incidents through normal behaviour / disciplinary procedures**
- **Ensure that members of the school community are aware that incidents have been dealt with**
- **Keep an 'E-Safety Incident Log' to keep a record of any incidents related to school and how they have been dealt with before feeding back to the Full Governing Body under the safeguarding item.**

Guidelines

Schedule for Development/Monitoring/Review

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

- *Logs of reported incidents*
- *SWGfL monitoring logs of internet activity (including sites visited)*
- *Surveys / questionnaires of*
  - *pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
  - parents / carers
  - staff

- The E-Safety policy will be reviewed annually
- Should serious E-Safety incidents occur, appropriate external agencies will be informed.

Education – Pupils

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.

- *All year groups will follow the 'South West Grid for Learning (SWGfL) – Digital Literacy' scheme of work for E-Safety as part of the ICT/PSHE curriculum. This should be regularly revisited to cover both the use of ICT and new technologies in school and outside school.*

- *Children from Year 6 will take on the role of 'Digital Leaders' to develop and maintain E-Safety within school. This will include tasks such as organising Safer Internet Day activities, newsletters, communicating advice to younger pupils and contributions to E-Safety related policies.*
- *Rules for safe internet use should be on display in every classroom*
- *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. (Hector the Protector)*
- *Where pupils are allowed to freely search the internet, eg 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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.*
- *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.*

Education – Parents/Carers

The school will seek to provide information and awareness to parents and carers through:

- **E-Safety Newsletters/advice in weekly school newsletters**
- **Distribution of publications by outside agencies e.g. Vodafone's Digital Parenting**
- **Parents' information evenings held at school**
- **Develop an E-Safety section of the school website**
- **Reference to the SWGfL Safe website (e.g. the SWGfL "Golden Rules" for parents)**

Education & Training – Staff

- *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 Policy before agreeing to it*
- *The E-Safety Coordinator will receive regular updates through attendance at SWGfL / LA training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required*

Training – Governors

Governors should take part in e-safety training as part of the wider safeguarding training offered by the school.

Technical – Infrastructure/Equipment, Filtering and Monitoring

- *School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and 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. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.*
- *All users will be provided with a username and password by the School Technician who will keep an up to date record of users and their usernames.*
- *The "master / administrator" passwords for the school ICT system, used by the Network Manager, must also be available to the Head teacher/ICT Coordinator and kept in a secure place*
- *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. (see password security appendix 8)*
- *The school maintains and supports the managed filtering service provided by EXA.*
- *In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher*
- *Any filtering issues should be reported immediately to EXA.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the ICT Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee*
- *School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy*
- *Remote management tools are used by staff to control workstations and view users' activity*
- *An appropriate system is in place for users to report any actual / potential E-Safety incident to the Network Manager.*

- *Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data*
- *An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system*
- *An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school*
- *An agreed policy is in place that allows staff to install programmes on school workstations / portable devices*
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users 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.*

Use of Digital and Video Images – Photographic, Video

- *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. 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 will not be used anywhere on a website or blog, particularly in association with photographs*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs of individual children are not to be used on the school website.*
- *Pupil's work can only be published with the permission of the pupil and parents or carers*

Data Protection

Staff must ensure that they:

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

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

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

Responding to incidents of misuse

- *Any incident of misuse should be reported to the E-Safety coordinator/Head teacher who in turn will take appropriate action.*

Conclusion

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

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

This e-safety policy helps 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.

Appendix 1:

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. A member of the Governing Body has taken on the role of *E-Safety Governor* and within this role meets with the E-Safety coordinator and monitors logs as necessary.

Head Teacher and Senior Leaders:

- *The Head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community, although the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator.*
- *The Head teacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant*
- *The Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The School Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.*
- *The Head teacher and another member of the School Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.*

E-Safety Coordinator/Officer:

- *Leads the E-Safety committee and tasks for Digital Leaders*
- *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 is aware of the procedures that need to be followed in the event of an E-Safety incident taking place.*
- *Provides training and advice for staff*
- *Liaises with the Local Authority*
- *Liaises with school ICT technical staff*
- *Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments,*
- *Meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs*
- *Attends relevant meeting / committee of Governors*
- *Reports regularly to School Leadership Team*

Network Manager/Technical Staff:

The ICT Technician / ICT Co-ordinator is responsible for ensuring that:

- *The school's ICT infrastructure is secure and is not open to misuse or malicious attack*
- *The school meets the E-Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance*
- *Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed*
- *EXA is informed of issues relating to the filtering applied by the Grid*
- *The school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- *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*
- *The use of the network / remote access / website / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Head teacher for investigation / action / sanction*
- *Monitoring software / systems are implemented and updated as agreed in school policies*

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*
- *Every year, they have read, understood and signed the school Staff Acceptable Use Policy (AUP)*
- *They report any suspected misuse or problem to the E-Safety Co-ordinator /Head teacher for investigation / action / sanction*
- *Digital communications with pupils (email / voice) should be on a professional level and only carried out using official school systems*
- *E-Safety issues are embedded in all aspects of the curriculum and other school activities*
- *Pupils understand and follow the school E-Safety and Acceptable Use Policy*
- *Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations*
- *They monitor ICT activity in lessons, extra-curricular and extended school activities*
- *They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices*
- *In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Designated Safeguarding Lead:

should be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from:

- *Sharing of personal data*
- *Access to illegal / inappropriate materials*
- *Inappropriate on-line contact with adults / strangers*
- *Potential or actual incidents of grooming*
- *Cyber-bullying*

E-Safety Committee:

Members of the *E-Safety committee* (to include the Head Teacher and a governor) will assist the *E-Safety Coordinator* with:

- *The production / review / monitoring of the school e-safety policy / documents*

- *The production / review / monitoring of the school filtering policy.*

Pupils:

- *Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign annually 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's 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. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- *Accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy*

Community Users:

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

Appendix 2

Staff Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That staff are protected from potential risk in their use of ICT in their everyday work.

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

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

I will be professional in my communications and actions when using school ICT systems:

- *I will 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, using official school systems e.g. Microsoft Outlook. 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) it will not be possible to identify by name, or other personal information, those who are featured*
- *I will not use chat and social networking sites in school*
- *I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. Email communication between staff and individual pupils is deemed inappropriate outside of learning purposes. Email communication with parents should only take place via the school administrator when face to face meetings / letters are not possible*
- *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. A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to school	X			
Use of mobile phones in lessons				X
Use of mobile phones in social time		X		
Taking photos on mobile phones or other camera devices				X
Use of hand held devices eg PDAs, PSPs	X			
Use of personal email addresses in school, or on school network		X		
Use of school email for personal emails				X
Use of chat rooms / facilities				X
Use of instant messaging				X
Use of social networking sites				X
Use of blogs			X	

- *When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. Personal use of such devices will only take place outside of lesson times and out of sight of children. Appropriate places to use personal devices include the staff car park, the back room of the library or the staff room.*
- *I will only access personal email accounts outside of school hours*
- *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 on a password protected flash drive or on the school network, in accordance with relevant school policies*

- *I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials*
- *I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work*
- *I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, other than programmes bought and licensed by the school, nor will I try to alter computer settings. The school technician should first verify any programmes/downloads required in addition to school programmes*
- *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 / LA Personal 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.

Name: …………………………………………………….

Signed: ……………………………………………………

Date: ……………………………………..

Appendix 3

Pupil Acceptable Use Policy Agreement KS2

Acceptable Use Policy Agreement

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

For my own personal safety:

- *I understand that the school will monitor my use of ICT*
- *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 share personal information about myself or others when on-line*
- *If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take a trusted adult with me*
- *I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable. (Hector the Protector)*

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

- *I understand that the school ICT systems are intended for educational use and that I will not use the systems for personal use unless I have permission to do so*
- *I will not try (unless I have permission) to make large downloads or uploads*
- *I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, 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 not access, copy, remove or alter any other user's files, without their knowledge and permission*
- *I will be polite and responsible when I communicate with others, I will not use 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 of the technology it offers me and to ensure the smooth running of the school:

- *I will only bring my personal hand held devices (mobile phones / USB devices etc) into school if I have permission. I understand that, if I do bring my own devices into school, I will hand the device into the school office at the beginning of the day and collect it at the end of the day. I understand that I must follow the rules set out in this agreement, in the same way as if I was using school equipment*
- *I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others*
- *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 who sent the email, due to the risk of the attachment containing viruses or other harmful programmes*
- *I will not 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 use chat and social networking sites.*

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

- *I should 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 disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.*

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 in school (when allowed) eg mobile phones, PDAs, cameras etc
- 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: …………………………………………….

Signed: …………………………………………… Date: …………………………………………..

Appendix 4

Pupil Acceptable Use Policy Agreement KS1

Acceptable Use Policy Agreement

- I will not talk to strangers on the internet.
- I will not tell anybody my full name, where I live or the school that I go to.
- If I find anything on the computer that worries me, I will click on Hector the Protector and tell my teacher.
- I will only use the computers for activities given to me by an adult.
- I will not visit websites that I don't have permission to visit.
- I will not change anybody else's work on the computer.
- I will only take photos of people with their permission.
- I will not bring my own computer games/phones into school.
- If ICT equipment is damaged then I will tell the teacher about it, however it happened.
- I will not try to change computer settings.

I understand that these rules are for my own safety and the safety of others. I understand that if I deliberately break these rules then the school may have to ban me from using the computers and speak to my parents/guardians.

I have read and understood the above and agree to follow the rules both in and out of school.

Name: …………………………………………….

Signed: …………………………………………… Date: ………………

Parent/Carer:

I have read through and discussed the acceptable use policy with my child.

Signed: ………………………………………

Appendix 5

Safe Use of the Internet KS2

Our School has installed computers and Internet access to help our learning.

These rules will keep everyone safe and help us to be fair to others:

- I must only use the Internet when an adult supervises me.
- If I find anything I'm uncomfortable with I will click on 'Hector the Protector' and tell the adult in charge.
- I will only e-mail people I know or that my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give out personal information or passwords.
- I will not arrange to meet anyone I don't know.
- I will not go on internet chat rooms or social networking sites.
- I will only use my own username and password and will not access other people's work without permission.

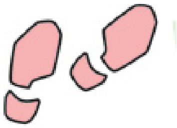
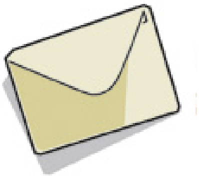
Any person abusing these guidelines will be denied free access to the ICT suite for a specified period of time and parents will be contacted.

Appendix 6

Safe Use of the Internet for KS1

Think then Click!

These rules help us to stay safe on the Internet:

	We only use the internet when an adult is with us.
	We can click on the buttons or links when we know what they do.
	We can click on Hector when we see something we don't like.
	We always ask if we get lost on the Internet.
	We can send and open emails together.
	We can write polite and friendly emails to people that we know.

Appendix 7

Pupil Sanctions – ICT Incidents

In the table below are possible incidents which would break the Pupil Acceptable Use Policy. The sanctions for these incidents have been suggested by the children. The degree to which the sanctions are enforced is at the class teacher's/Head teacher's discretion and likely to alter according to the severity of the incident.

	Reduction in computer time	Not allowed to work individually on computers	Missing Playtime	Restricted use e.g. only allowed to visit selected websites	Internet ban	Full computer ban	Report to the Head Teacher	Contact Parents	Suspension	Police involvement
Using mobile phone in school	X									
Accessing inappropriate websites		X	X							
Hacking user accounts			X	x						
Downloading / Installing without permission				X						
Giving out personal information					X			X		
Talking to strangers						X				
Cyberbullying						X	X	X		
Hacking into the school server						X	X			
Accessing illegal websites								X	X	X

Appendix 8

School Password Security

The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email.

Responsibilities:
The management of the password security policy will be the responsibility of the E-Safety Coordinator.

All children from Y3 and above and adults will have responsibility 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. Children in EYFS and KS1 will be provided with 'class log-ins'.

Passwords for new users and replacement passwords for existing users will be allocated by technical support or the E-Safety Coordinator.

The following rules apply to the use of passwords:

EYFS/KS1 Users:

- *All users will be provided with a class log-in to be used for all computer suite activities*

KS2 Users – Y3 and Y4:

- *passwords must be changed at the beginning of terms 1 and 4*
- *the password should be a minimum of four characters long and*
- *must include at least one upper case letter and one number*
- *must not include proper names*

KS2 Users – Y5 and Y6:

- *passwords must be changed at the beginning of terms 1, 3 and 5*
- *the password should be a minimum of six characters long and*
- *must include at least one uppercase letter, one lowercase character, one number and one special character e.g. % £ # @*
- *must not include proper names*

Adult Users:

- *passwords to be changed at the user's discretion (due to user ID being required for laptop network access)*
- *the password should be a minimum of eight characters long and*
- *must include at least one uppercase letter, one lowercase letter, one number and one special character e.g. # @ * %*
- *must not include proper names*

All Users:

- *the account should be "locked out" following three successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *requests for password changes should be authenticated by the E-Safety Coordinator to ensure that the new password can only be passed to the genuine user*

Training / Awareness:

Members of staff will be made aware of the school's password policy:

- through the school's e-safety policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in ICT and / or E-Safety lessons
- through the Acceptable Use Agreement

Policy Statements:

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee (or other group).

The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).

Audit / Monitoring / Reporting / Review:

The E-Safety Coordinator will ensure that full records are kept of security incidents related to this policy. In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.