ST JOHN'S CATHOLIC INFANT SCHOOL

E-Safety/ Online Safety Policy

"Loving, Learning and Laughter Together with God"

Article 3: "The best interests of the child must be top priority in all actions concerning children"

"*Our children will know more, can remember more and apply more*"

Contents

Appendices:

- Pupil Acceptable Use Policy Agreement Template – older children
- Pupil Acceptable Use Policy Agreement Template – younger children
- Parents / Carers Acceptable Use Policy Agreement Template
- Staff and Volunteers Acceptable Use Policy Agreement Template
- FS/KS1 E-Safety Rules
- School Technical Security Policy template (includes password security and filtering)
- Legislation
- Links to other organisations and documents
- Glossary of Terms

Development / Monitoring / Review of this Policy

This E-Safety policy has been developed by consultation with

- Headteacher / Senior Leaders
- Computing Lead and Subject Leaders
- Staff – including Teachers, Support Staff, Technical Staff
- Governors
- Parents and Carers

Schedule for Development / Monitoring / Review

This E-Safety policy was approved by the Governing Body / Governors Sub Committee on:	27th July 2018
The implementation of this E-Safety policy will be monitored by the: Hi Impact, SLT and the computing lead.	Computing Lead – Emma Greer Technician – Megan Jones Senior Leadership Team
Monitoring will take place at regular intervals:	Termly
The E-Safety Policy will be reviewed annually by staff and Governors, 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 review date will be :	Summer 2022

Scope of the Policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.
The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). In the case of both acts, action may only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities 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 Curriculum Committee receiving information about E-Safety incidents as and when they occur.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community; the day to day responsibility for E-Safety will be delegated to all SLT.
- The Headteacher and the other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. (see flowchart on dealing with E-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR).
- The Headteacher / Senior Leaders are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher / 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.

Computing Lead:

- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school ESafety 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 or outsources training and advice for staff
- liaises with the Local Authority if necessary
- liaises with technical support staff
- receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments,
- attends relevant training
- reports to other members of the Senior Leadership Team if E-Safety issues occur

Hi-Impact Technical staff:

Technical Staff for Computing are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required E-Safety technical requirements and any statutory guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed where and when appropriate.
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep 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.
- that the use of the network / internet / Virtual Learning Environment / Twitter/remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Computing Lead for investigation / action / sanction. The approach needs to be evaluated regularly in light of new developments and methods.

Teaching & 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 Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; Computing Lead for

investigation/ action / sanction.
• all digital communications with pupils / parents / carers 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 activities
• pupils understand and follow the E-Safety and acceptable use policies
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current 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 / safeguarding 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

Children:

• are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
• 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 policies on the use of mobile devices and digital cameras. They should also know and understand 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.
• will experience E-Safety training as part of their curriculum each year.

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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / Twitter/ local E-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:
• digital and video images taken at school events
• access to parents' sections of the website / VLE and on-line / pupil records

Students/Work Experience/Volunteers/Community Users

Students/Work Experience/Volunteers/Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA (Acceptable Use Agreement) before being provided with access to school systems.

Policy Statements

Education – children

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 should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned E-Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
• 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
• Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
• Staff should act as good role models in their use of digital technologies the internet and mobile devices
• in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
• Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and insist in the use of safe search engines.
• It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should give clear reasons for the need.

Twitter

Twitter School Aims

- To quickly share and celebrate children's achievements, successes and school updates.
- To demonstrate safe and responsible use of social media To encourage the use of 21st Century technology

St John's Catholic Infant School Twitter accounts have been set up for the purpose of distributing administrative messages, and promoting school activities and achievements. The school Twitter account will post photos of work and learning and may include children's faces For example we may share a photo of a child creating a piece of artwork that features the child's hands or back of the head. If the child's face is used there will be no reference to their name. Parents can opt out of this at any time and all staff should be made aware of children whose photographs cannot be used.

Education – parents / carers

Many parents and carers have 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

• Curriculum activities
• Letters, newsletters, website, parentmail, Twitter
• Parents / Carers evenings / sessions
• High profile events / campaigns eg E-Safety workshops for parents and children
• Reference to the relevant web sites / publications eg www.saferinternet.org.uk/ http://www.childnet.com/parentsand-carers (see school website and appendix for further links / resources)

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's ESafety knowledge and experience. This may be offered through the school website providing E-Safety information for the wider community.

Education & Training – Staff / Volunteers

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:

- 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 Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Computing Lead will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the previous sections will be effective in carrying out their E-Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted (Server Room).
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by in house technical support who will keep an up to date record of users and their usernames. Staff users are responsible for the security of their username and password and will be required to change their password where and when appropriate.
- 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.
- The technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content is filtered by the broadband/filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored by broadband provider.

A filtering system called Surf Protect also supports the monitoring of internet usage. This enables school to:

- View which websites are being accessed / requested in real time.
- View a historical log of all website requests, searchable by date.
- Export any key data to a CSV file, to store it on a computer for use when required.
- View graphical representations of your school's Internet usage, e.g. the top 5 blocked websites by percentile.
- Search by username or website; helpful for students with particular cause for concern.
- See an overview of the school's Internet usage – e.g. which sites are most frequently visited or blocked – providing an insight into the role that connectivity services plays as an educational tool.
- This tool can also support the Prevent agenda in monitoring websites that promote terrorism and terrorist ideologies, violence or intolerance

- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (see appendix)
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- 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 school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing

programmes on school devices.
• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail).

Use of digital and video images

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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for Cyber Bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
• Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Pupils must not take, use, share, publish or distribute images of others without their permission.
• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
• Pupils' full names 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 or school twitter account
• Pupil's work can only be published with the permission of the / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:
• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate
• Kept no longer than is necessary
• Processed in accordance with the data subject's rights
• Secure
• Only transferred to others with adequate protection.

The school must ensure that:
• It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
• Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
• All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
• It has a Data Protection Policy (see appendix for template policy)
• It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
• Risk assessments are carried out
• It has clear and understood arrangements for the security, storage and transfer of personal data
• Data subjects have rights of access and there are clear procedures for this to be obtained
• There are clear and understood routines for the deletion and disposal of data

- There is a clear routine for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

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, memory 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 data must be securely deleted from the device, once it has been transferred or its use is complete.

Communications

When using communication technologies the school considers the following as good practice:
- The official school email service may be regarded as safe and secure.
- Users must immediately report, to the nominated person the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems.

Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils should be taught about E-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/ and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Computing lead to ensure compliance with the E-Safety policy.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below should not encourage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows :-

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sits, make, post, download, upload, data transfer, communicate or pass on,	Child sexual abuse images – The making, production or distribution of indecent images of children contrary to the					

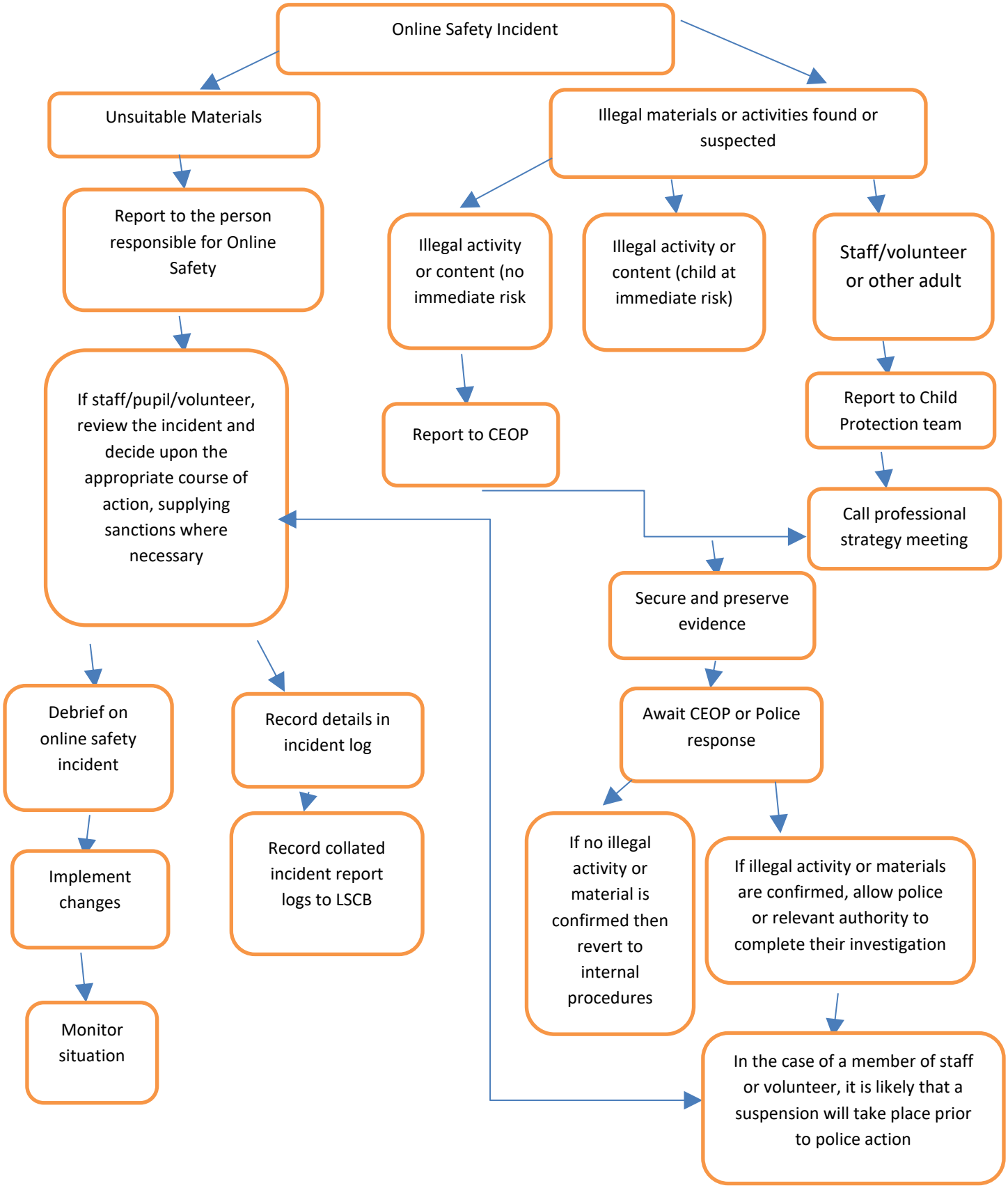
materials, remarks, proposals or comments that contain or relate to :	Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the Internet)					X	
Online Gaming					X	
Online Gambling					X	
Online shopping/commerce			X			
File sharing				X		
Use of social media			X			
Use of messaging apps			X			
Use of video recording, ie You Tube			X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" on previous page).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal activity or content (no immediate risk
Illegal activity or content (child at immediate risk)
Staff/volunteer or other adult
If staff/pupil/volunteer, review the incident and decide upon the appropriate course of action, supplying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Debrief on online safety incident
Record details in incident log
Await CEOP or Police response
Implement changes
Record collated incident report logs to LSCB
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
    - If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

This policy will be reviewed at least every two years or sooner if necessary.

The governing body have wider responsibilities under the Equalities Act 2010 and will ensure that all our school policies take account of the nine protected characteristics. We strive to do the best for all of the children and staff irrespective of age, disability, educational needs, race, nationality, ethnic or national origin, pregnancy, maternity, sex, gender reassignment, religion/belief, marriage/civil partnership or sexual orientation or whether they are looked after children.

We have carefully considered and analysed the impact of our policies on equality and the possible implications for pupils with these protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Agreed by Governors on: 3rd November 2016	**Reviewed on:** 18th November 2021 19th November 2020 (Min No 14/20)	 15th November 2018 (Min No 20/18) 2nd November 2017 (Min No: 33/17)

APPENDICES

- Pupil Acceptable Use Agreement template (KS2 children)
- Pupil Acceptable Use Agreement template (F2/KS1 children)
- Parents / Carers Acceptable Use Agreement template
- Staff and Volunteers Acceptable Use Agreement Policy template
- F2 and KS1 E-Safety Rules
- E Safety Rules for school visitors
- School Technical Security Policy template including Filtering
- School Privacy Notice
- Legislation
- Links to other organisations and documents
- Glossary of terms

Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers or ipads
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer or ipad.

Signed (child):……

Signed (parent): ……..

Parent / Carer
Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

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 systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
• that parents and carers are aware of the importance of E-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name ……

Pupil's name ……

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

(KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, E-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

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

Signed …….. Dated ……

St John's Catholic Infant School
Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, ipads, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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/Twitter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

• When I use my mobile devices (ipads / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
• I will ensure that my data is regularly backed up.
• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
• I will not 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, nor will I try to alter computer settings.
• I will not disable or cause any damage to school equipment, or the equipment belonging to others.
• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/ LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local 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 the 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 off the premises and my use of personal equipment on the premises 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 / Directors 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 name ……

Staff signature ……

Dated ……

St John's Catholic Infant School's
Foundation Stage and KS1 E-Safety Code

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 search the Internet with an adult.
	We always ask if we get lost on the internet

St John's Catholic Infant School's
E- Safety Rules for School Visitors

Please follow our eSafety rules during school time

	All mobile phones should be switched off when entering the children's working areas.
	No photographic or video equipment is to be used unless authorized by the school.

Dispensation may be given in certain circumstances at the discretion of the Headteacher.

Thank you for your assistance

School Technical Security Policy
(Including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. 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 (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled
- logs are maintained of access by users and of their actions while users of the system.
- there is effective guidance and training for users.
- there are regular reviews and audits of the safety and security of school computer systems.
- there is oversight from senior leaders and these have impact on policy and practice.

As the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the E-Safety measures that might otherwise be carried out by the school itself (as suggested below). It is also important that the managed service provider is fully aware of the school E-Safety Policy /Acceptable Use Agreements. The school will also check the Local Authority / other relevant body policies / guidance on these technical issues.

Responsibilities

The management of technical security will be the responsibility of Hi-Impact and their staff, and Melanie Raynor (Computing Lead).

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually.
- 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 section below).
- Hi-Impact are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- 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 technical incident to the Computing

Co-ordinator, Headteacher or Technician.
• An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users.
• An agreed policy is in place regarding the extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school.
• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. (see School Personal Data Policy Template in the appendix for further detail)
• The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail).

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

● All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually.
● All school networks and systems will be protected by secure passwords that are regularly changed.
● The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader
● Passwords for new users, and replacement passwords for existing users will be allocated by our Technician . Any changes carried out must be notified to the manager of the password security policy (above).
● All users (adults and young people) 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.
● Users will change their passwords at regular intervals – as described in the staff and pupil sections below.
● The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account.
● Requests for password changes should be authenticated by our Hi Impact to ensure that the new password can only be passed to the genuine user

Staff passwords:

● All staff users will be provided with a username and password by our Technician who will keep an up to date record of users and their usernames.
● the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
● must not include proper names or any other personal information about the user that might be known by others
● the account should be "locked out" following six successive incorrect log-on attempts
● temporary passwords e.g. used with new user accounts or when users have forgotten 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)
● passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
● should be changed at least every 60 to 90 days.
● should not re-use for 6 months and be significantly different from previous password the last four passwords cannot be re-used passwords created by the same user.
● should be different for systems used inside and outside of school.

Pupil passwords

● All users (at KS1/2 and above) will be provided with a username and password by our Hi Impact Technician

who will keep an up to date record of users and their usernames.
- Users will be required to change their password regularly.
- Pupils will be taught the importance of password security.
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:
- at induction.
- through the school's E-Safety policy and password security policy.
- through the Acceptable Use Agreement.

Pupils will be made aware of the school's password policy:
- in lessons.
- through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The responsible person will ensure that full records are kept of:
- User Ids and requests for password changes.
- User log-ons.
- Security incidents related to this policy.

Legislation

School is 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 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-andconfiscation

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website: http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducingbureaucracy/requirements/changestoschoolinformationregulations

Links to other organisations or documents

The following links may help those who are developing or reviewing a school E-Safety policy.

UK Safer Internet Centre

Safer Internet Centre -
Childnet
Professionals Online Safety Helpline
Internet Watch Foundation

CEOP

http://ceop.police.uk/
ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis
Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government Better relationships, better learning, better behaviour
DCSF - Cyberbullying guidance
DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies
Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Alberta, Canada - digital citizenship policy development guide.pdf
Teach Today – www.teachtoday.eu/
Insafe - Education Resources
Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note – BYOD

Data Protection

Information Commissioners Office:
Your rights to your information – Resources for Schools - ICO
ICO pages for young people
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)
E-Safety Policy
50 | Page
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO – Access Aware Toolkit
ICO - Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
SWGfL - Guidance for Schools on Cloud Hosted Services
LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data
NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People
Kent - Safer Practice with Technology
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - Questions for Technical Support
NEN - Guidance Note – Esecurity

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum
SWGfL BOOST Presentations - parents presentation
Connect Safely - a Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
DirectGov - Internet Safety for parents
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consorti) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
TUK	Think U Know – educational E-Safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol