ST MARGARET OF SCOTLAND CATHOLIC PRIMARY SCHOOL

E-SAFETY POLICY

Learning with Jesus in

Faith Hope and Love

E-Safety Policy

Appendices

Learning with Jesus in Faith, Hope and Love.
Background and Rationale

At St Margaret of Scotland Catholic Primary School we recognise and celebrate that each child is made in the image of God and as a response to God's invitation, encourage each individual to develop to the best of his/her ability. The use of new technologies has become integral to the lives of our children, both within school and in their lives outside school and we seek to use these in a safe way to promote learning and a respect for one another.

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

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

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

Many of these risks reflect situations in the off-line world and this e-safety policy is used in conjunction with other school policies. This policy should be read alongside the school's Anti-bullying Policy, Behaviour Policy, Safeguarding Policy and Equality Policy.

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 explains how we intend to safeguard and ensure we do everything that is reasonably expected to manage and reduce risks, in order to help young people, staff and their parents / carers to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by the IT Manager and reviewed by Headteacher / Senior Leaders, Staff, Governors, Parents and Carers.

Monitoring will take place at regular intervals.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Should serious e-safety incidents take place, the following external persons / agencies should be informed - LSCB Local Authority Designated Officer, Luton IAT.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, staff, parents and carers

The e-Safety Policy was revised by: …………………………………..

It was approved by the Governors on: ……………………………….

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

Roles and Responsibilities

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

Governors

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

- regular meetings with the E-Safety Co-ordinator / IT Manager
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting
- review and approval of the e-safety policy

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the IT Manager.
- The Headteacher / Senior Leaders are responsible for ensuring that the IT Manager and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

- The Headteacher / 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.
- The Senior Leadership Team / Senior Management Team can request monitoring reports from the IT Manager.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

ICT Manager

The ICT Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack, and any misuse needs to be reported to the schools Senior Leaders.
- that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy.
- keeping 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
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- providing & arranging training and advice for staff
- liaising with the Local Authority
- reporting regularly to Senior Leadership Team.
-

E-Safety Coordinator

The role of the E-Safety coordinator will include:

- taking day-to-day responsibility for e-safety issues and a leading role in establishing and reviewing the school e-safety policies and documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- providing training and advice for staff
- liaising with the Local Authority
- reporting regularly to Senior Leadership Team.

Teaching and Support Staff

All staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy Agreement

- they report any suspected misuse, cyberbullying or problem to the a senior member of staff for investigation / action / sanction
- digital communications with pupils, e.g. email, Learning Platform, 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 person for child protection

The Designated person for child protection 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

N.B. these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Pupils

All pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- should develop 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 and carers will be responsible for:

- endorsing, by signature, the Parent and Carers Acceptable Use Policy Agreement
- reporting any suspected misuse, cyber bullying or problem their child's teacher or a Senior member of staff for investigation / action / sanction.

Community Users

Community Users who access school ICT systems, websites & Learning Platform etc as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Community access may be restricted by discretion of the IT Manager to protect the Security, Integrity and reliability of the schools network for Teaching and Learning.

Policy Statements

Education – pupils

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

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

- a planned e-safety programme, covering both the use of current and new technologies in school and outside school, is provided appropriate to age across the curriculum
- key e-safety messages are reinforced as part of a planned programme of assemblies
- pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of the internet and mobile devices both within and outside school
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- advice and guidance for use of ICT systems and the internet are posted in all rooms
- staff should act as good role models in their use of all technologies and the internet.

Education – 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, Learning Platform and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice by:

- endorsing, by signature, the Parent and Carers Acceptable Use Policy Agreement
- reporting any suspected misuse, cyber bullying or problem their child's teacher or E-Safety Co-ordinator for investigation / action / sanction.

They will also be encouraged to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- personal devices in the school (where this is allowed)

Education - Extended Schools

The school does offer family learning courses in, for example, ICT, media literacy and e-safety so that parents and children can gain a better understanding of these issues. Messages around e-safety are also targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy using a range of different technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

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.

- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students 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 temporarily remove those sites from the filtered list for the period of study from E2BN. Any request to do so should include clear reasons for the need. Staff will also need to inform the IT Manager when contacting E2BN.

All staff will receive e-safety training and need to understand their responsibilities, as outlined in this policy. Training is offered as follows:

- a planned programme of formal e-safety training is made available to staff. An audit of the e-safety training needs of all staff will be carried out twice a year. It is expected that some staff will identify e-safety as a training need within the performance management process.
- all new staff will be talked through the school e-safety policy and Acceptable Use Policies as part of their induction programme
- the IT Manager or IT Staff will receive regular updates through attendance at LSCB training sessions and by reviewing guidance documents released by LSCB

- this E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- the IT Manager will provide advice / guidance / training as required to individuals as required

E-Safety Group

The school is in the process of establishing an E-Safety group. The E-Safety Group will provide a consultative group with wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body / Directors.

- Members of the E-safety Group 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 and requests for filtering changes.
- Mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring network / internet / incident logs.
- Consulting stakeholders – including parents / carers and the pupils about the e-safety provision
- Monitoring improvement actions identified through use of the 360 degree safe self review tool

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members involved in ICT, e-safety, health and safety, child protection. This is offered in a number of ways:

- attendance at training provided by the LSCB, LBC or other relevant organisation.
- participation in school training / information sessions for staff or parents

Technical – infrastructure, equipment, filtering and monitoring

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

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the nature of the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school, LBC or the LSCB can accept liability for any materials accessed, or any consequence of Internet access.
- The school uses the fully tested, accredited Protex web filtering service provided by E2BN.
- There are 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 ICT Manager and will be reviewed, termly. All requests for access beyond that normally allocated (e.g. access to the schools MIS) shall be authorised by the SLT and where necessary the governing body. This shall include the authorisation of access required by the ICT Support Team during investigations. Where 'restricted' information is stored, access shall only be granted to individuals approved by the SLT. Please see the finance manual for details on restricted access to Finance Systems.
- Access to all ICT systems is via unique login and password. Any exceptions shall be guidance in the risk assessment, and approved by the SLT. All users will be provided with a username and password by the ICT Manager who will keep an up to date record of users and their usernames. Users will be required to change their passwords on a regular bases, see password policy below.
- The administrator passwords for the school ICT system, used by the ICT Manager is also be available to the Headteacher 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.
- The school ICT Manager can regularly monitors the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. All school ICT activity and on-line communications including any personal and private communications made via the school network may be monitored,
- Remote management tools are used by the ICT Manager to control and view the school server.
- The IT Support staff will use a mobile device management system to track, maintain and monitor the use of Mobile assets, Mobile assets include but are not limited to school Laptops and Tablet Devices.
- An appropriate system is in place for users to report any actual / potential e-safety incident to a senior member of staff.
- 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 for starters and leavers. The Admin Team shall ensure that the ICT Manager is informed promptly of any member of staff joining or leaving the school. Any school owned ICT equipment should be returned to the ICT Manager when staff leave. The ICT Manager shall ensure that leavers' access is disabled, in a timely manner. There is a similar process for pupils starting or leaving the school.
- An agreed policy is in place regarding the downloading of executable files by users, installing programmes on school workstations and portable devices and use of removable media (eg memory sticks / CDs / DVDs)
- The school will ensure all data is backed-up on a daily basis. A data backup is automated, taken at regular intervals (daily) but remains in a separate building to the original data store. Additionally a backup is done once per week to account for disaster . Backup media is subject to destruction procedures as other ICT storage devices.

- The school infrastructure and individual workstations are protected by up to date virus software.

Passwords

Passwords are an important aspect of information security, and are the usual way to protect access to information. As such, all members of staff with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords. These steps should include:

- Keeping their password secure from pupils, family members, and other staff
- Using a different password for accessing school systems to that used for personal (non-school) purposes
- Choosing a password that is difficult to guess, or difficult for pupils to obtain by watching staff login
- Adding numbers or special characters (e.g. !@£$%^) can help
- Changing passwords regularly e.g. each school term
- Staff should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else
- In addition, when leaving a computer for any length of time, all staff shall log off or lock the computer, using CTRL+ATL+DELETE (Computers will automatically lock after 45 minutes).
- Ensuring that there is a limit on the number of consecutive failed log in attempts. (Best practice is between 3 and 5 attempts)
- Restrict concurrent access i.e. a user should not be able to log in at the same time from two different machines.
- Password changes are enforced every 7 weeks (approx. each half term)
- Passwords children use are appropriate to their age and the complexity should increase as children progress through the school. e.g. Year1 might have dog
- Administrator passwords are changed in accordance with staff password polices but administrator password complexity has a minimum of 8 characters.

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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Images should only be taken on school equipment unless approval is sought from the IT Manager where school memory storage will be provided. All images should be downloaded to the school system and removed from the device at the earliest opportunity and images should not leave the premises.
- 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.
- Pupil's full names will not be used anywhere on the school website or Learning Platform, particularly in association with photographs.
- Written permission from parents or carers is obtained as part of the AUP signed by parents or carers annually.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Images of pupils should only be kept while a pupil is on roll, old images need to be deleted and removed from the recycle bin additionally unwanted paper imagery should be shredded . Images of pupils should always be removed from portable devices at the earliest opportunity.

- Images of staff can be taken for promotional purposes and used to promote the school however a member of staff has permission to object to a photo being used and can ask for it to be removed.

Data Protection

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

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- kept no longer than is necessary
- processed in accordance with the data subject's rights
- secure
- only transferred to others with adequate protection.

Staff must ensure that they:

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

When confidential 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 school uses bitlocker on at risk devices and communicates confidential data using egress email.

- The device must be password protected (most memory sticks can be password protected by the IT Manager on request)
- Passwords and encryption keys should not be written down unless absolutely necessary. Where passwords are recorded they must not be stored with the associated device.
- 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.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Any digital communication between staff, pupils, parents and carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

- When using communication technologies the school considers the following as good practice:
  - the official school email service (stmargarets.luton.sch.uk) is regarded as safe and secure and is monitored. Users should be aware that email and communications are monitored. However we recommend that staff ensure that all confidential documents, text or attachments are sent in an encrypted format.
  - Staff must not give out their personal email address to pupils or parents, communication from parents should be directed to the schools generic admin email account admin@stmargarets.luton.sch.uk
  - Pupil or Class email accounts can be setup on request to aid in the teaching and learning of communication technologies. These accounts will be closely checked and monitored by school staff.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email. Emails must not be deleted but kept as evidence.
- Pupils should be taught about safety issues, such as the risks attached to the use of personal details when using different forms of communications e.g. email, messages, text etc. They should also be taught strategies to deal with inappropriate emails, messages etc. and be reminded of the need to write clearly and correctly and not include any unsuitable or abusive material. The reason for this is that many pupils use Message systems over email.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Videoconferencing should use the schools broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call. Teachers should inform the ICT Manager before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

- All calls to parents, carers and pupils must be made via the school telephone system. Staff must not contact parents, carers or pupils using their personal mobile phones and must not give out mobile numbers to pupils, parents or carers unless discussed with the Headteacher first.
- Users of mobile telephones sign and agree to the Luton Borough Council Policy & Procedure for the use of Telephones.
- Mobile phones provided by the school do not have cameras to prevent allegations against members of staff. Additionally any smartphone devices purchased for school use will have the camera disabled or removed.

The following shows how the school currently considers the benefit of using a range of technologies for education outweighs their risks / disadvantages. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

•Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
•Clear reporting guidance, including responsibilities, procedures and sanctions
•Risk assessment, including legal risk

School staff should ensure that:

•No reference should be made in social media to students / pupils, parents / carers or school staff
•They do not engage in online discussion on personal matters relating to members of the school community
•Personal opinions should not be attributed to the school /academy or local authority
•Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

For further information see the schools social networking policy.

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

Unsuitable and 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 engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*
	pornography				*	
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred				*	
	threatening behaviour, including promotion of physical violence or mental harm				*	
	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				*	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Using school systems to run a private business				*	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LBC and / or the school				*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				*	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				*	
Creating or propagating computer viruses or other harmful files				*	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				*	
On-line gaming (educational)	*				
On-line gaming (non educational)			*		
On-line gambling				*	
On-line shopping / commerce			*		
Sharing of royalty and copyright free resources	*				
Use of video broadcasting e.g. uploading to Youtube (educational)			*		

Responding to incidents of misuse

An important element of e-Safety is the ability to identify and deal with incidents related to the confidentiality of information. All staff and pupils have a responsibility to report e-Safety or e-Security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the school. It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse.

If any apparent or actual misuse appears to involve illegal activity i.e:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The LSCB flow chart, see appendices section, should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

Any incidents will be dealt as soon as possible in a proportionate manner, however members of the school community might not always be aware of the outcome.

If a member of staff has a concern over the safety or wellbeing of a child, this should be reported to your designated safeguarding officer using school polices.

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 (appendix) for responding to online safety incidents and report immediately to the police.

It is intended that incidents of misuse will be dealt with through normal behaviour and disciplinary procedures as follows:

Pupils	**Actions / Sanctions**								
Incidents:	Refer to class teacher	Refer to Phase Leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			*	*					
Unauthorised use of non-educational sites during lessons	*	*	*						
Unauthorised use of mobile phone / digital camera / other handheld device			*						
Unauthorised use of social networking / instant messaging / personal email			*						
Unauthorised downloading or uploading of files			*		*				
Allowing others to access school network by sharing username and passwords	*	*			*	*		*	
Attempting to access or accessing the school network, using another student's / pupil's account	*	*	*		*	*	*		*
Attempting to access or accessing the school network, using the account of a member of staff		*	*		*	*	*		*
Corrupting or destroying the data of other users		*	*		*	*			*

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			*			*	*		*
Continued infringements of the above, following previous warnings or sanctions			*			*	*		*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			*			*	*		*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*			*	*			
Deliberately accessing or trying to access offensive or pornographic material		*	*	*	*	*	*		*
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	*	*				*		*	

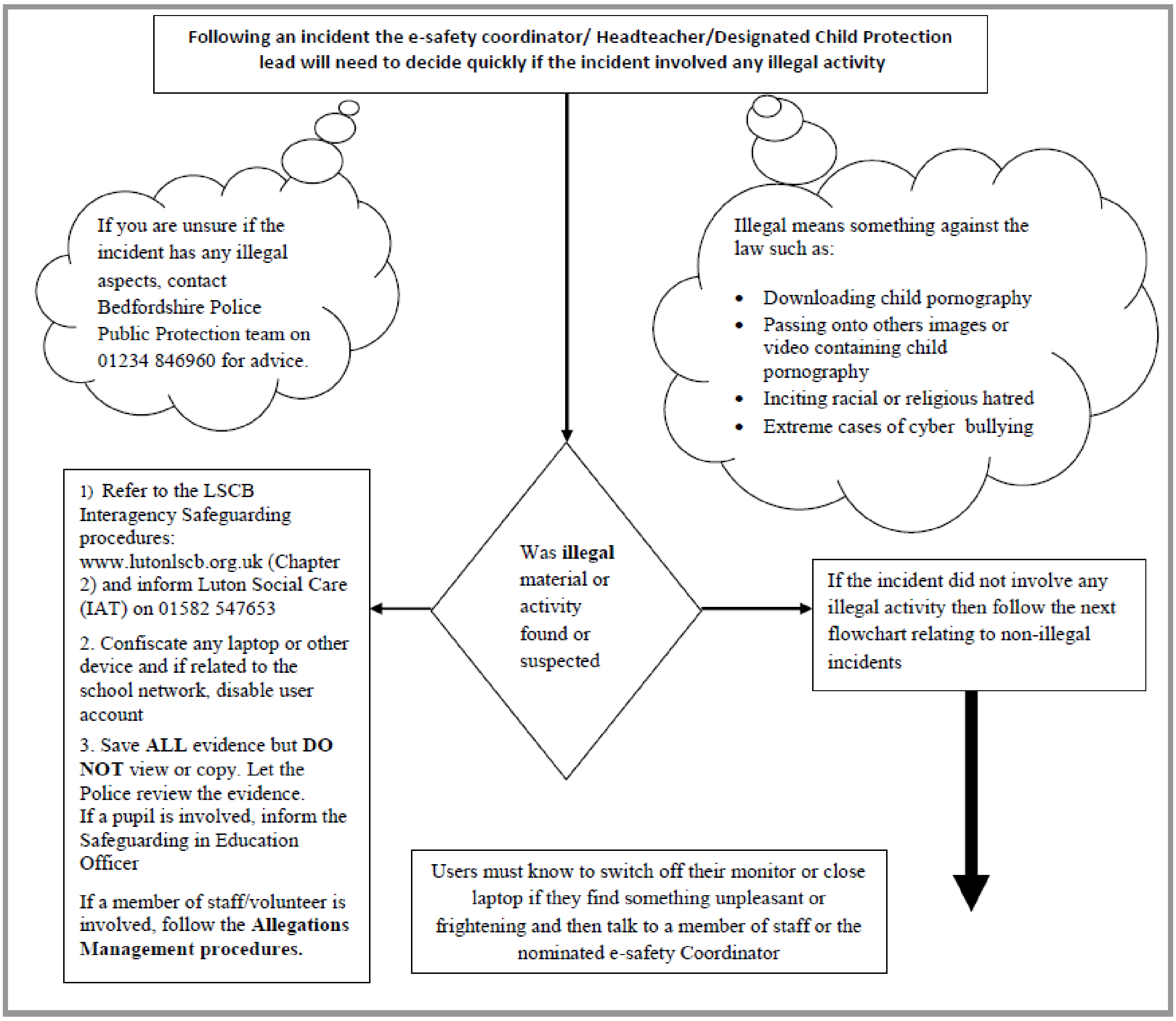
Staff **Actions / Sanctions**

Incidents:	Refer to line managerr	Refer to Headteacher	RRefer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		*	*	*				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	*	*				*		
Unauthorised downloading or uploading of files	*				*	*		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account					*	*		
Careless use of personal data eg		*	*			*		

holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules		*	*		*			*
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		*	*	*				*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		*	*	*				*
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		*	*	*		*		
Actions which could compromise the staff member's professional standing		*	*					*
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		*	*					*
Using proxy sites or other means to subvert the school's filtering system		*			*	*		
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*			*	*		
Deliberately accessing or trying to access offensive or pornographic material		*	*	*			*	*
Breaching copyright or licensing regulations	*	*				*		
Continued infringements of the above, following previous warnings or sanctions		*	*				*	*

Appendix A.

Luton Flowchart to support decisions related to an illegal e-safety incident.



Following an incident the e-safety coordinator/ Headteacher/Designated Child Protection lead will need to decide quickly if the incident involved any illegal activity

If you are unsure if the incident has any illegal aspects, contact Bedfordshire Police Public Protection team on 01234 846960 for advice.

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of cyber bullying

Was **illegal** material or activity found or suspected

1) Refer to the LSCB Interagency Safeguarding procedures: www.lutonlscb.org.uk (Chapter 2) and inform Luton Social Care (IAT) on 01582 547653

2. Confiscate any laptop or other device and if related to the school network, disable user account

3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence.
If a pupil is involved, inform the Safeguarding in Education Officer

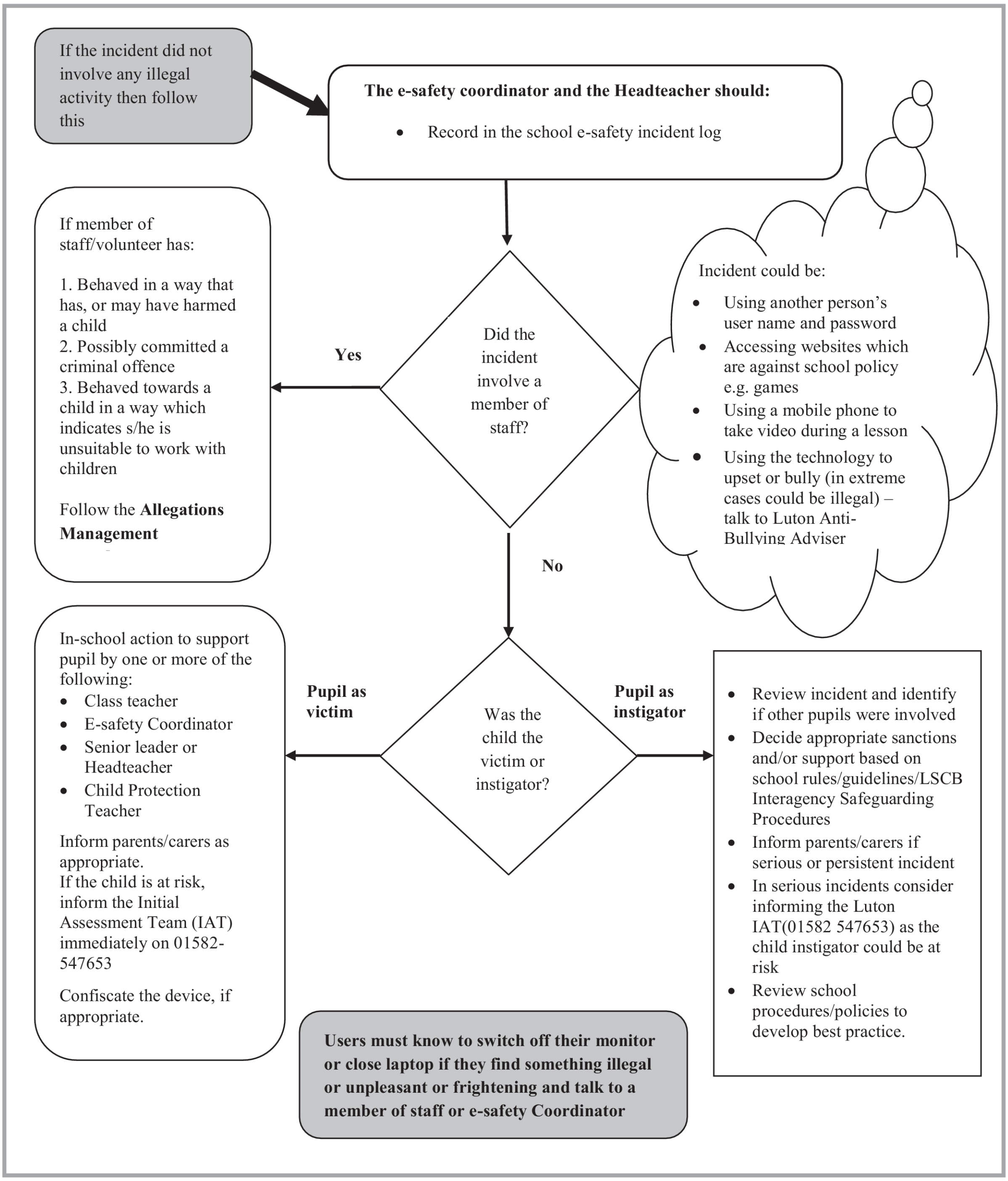
If a member of staff/volunteer is involved, follow the **Allegations Management procedures.**

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the nominated e-safety Coordinator

Appendix B.

Luton Flowchart to support decisions related to non-illegal e-safety incident.



If the incident did not involve any illegal activity then follow this

The e-safety coordinator and the Headteacher should:

- Record in the school e-safety incident log

Did the incident involve a member of staff?

Yes

If member of staff/volunteer has:

1. Behaved in a way that has, or may have harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children

Follow the **Allegations Management**

Incident could be:

- Using another person's user name and password
- Accessing websites which are against school policy e.g. games
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Luton Anti-Bullying Adviser

No

Was the child the victim or instigator?

Pupil as victim

In-school action to support pupil by one or more of the following:

- Class teacher
- E-safety Coordinator
- Senior leader or Headteacher
- Child Protection Teacher

Inform parents/carers as appropriate.
If the child is at risk, inform the Initial Assessment Team (IAT) immediately on 01582-547653

Confiscate the device, if appropriate.

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/or support based on school rules/guidelines/LSCB Interagency Safeguarding Procedures
- Inform parents/carers if serious or persistent incident
- In serious incidents consider informing the Luton IAT(01582 547653) as the child instigator could be at risk
- Review school procedures/policies to develop best practice.

Users must know to switch off their monitor or close laptop if they find something illegal or unpleasant or frightening and talk to a member of staff or e-safety Coordinator

Acknowledgements

SWGfL holds copyright of this document, consent has been given to adapt and use resources.