In the Light of Jesus
we Learn to Shine

St. Joseph's Catholic Primary School

Online Safety Policy

Ratified by Governors

Date: 18.03.24

Document Status	
Reviewed	March 2024
Date of next Review	March 2025
Approval Body	Governing Body
Publication	School Website/Staff Policy folder

This policy must be reviewed annually

We have carefully considered the impact of this policy on equality and the possible implications for pupils with 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.

This online safety policy should be read in conjunction with our:

- Safeguarding & Child Protection Policy
- Behaviour & Discipline Policy
- Social Media Policy
- Anti-Bullying Policy
- Data Protection Policy, Privacy Policy and Privacy notice
- School's Code of Conduct

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

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.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online 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 online safety behaviour that takes place out of school.

Schedule for Development / Monitoring/ Review

This online safety policy was approved by the *Governing Body / Governors Sub Committee in:*	March 2024
The implementation of this online safety policy will be monitored by the:	*Governors, SLT, Network Manager, Class Teachers*
Monitoring will take place at regular intervals:	*At least annually or more frequently if required.*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*annually*
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	March 2025
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager,* *LA Safeguarding Officer,* *Police Commissioner's Office*

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS)
- Termly reports will be produced on CPOMs and monitored by the Headteacher. These will be presented to the Full Governing Body.
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

Acknowledgement

- This policy is based on the model policy from the South West Grid for Learning Trust (SWGfL).

Roles & Responsibilities

Governors

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

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of Online Safety incident logs (CPOMs)
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- **The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community**; though the day-to-day responsibility for online safety will be delegated to Year Leaders and class teachers.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online 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 online safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles, within LA guidelines for schools.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.
- **The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.**

Online safety Coordinator:

The school has appointed an Online Safety Co-ordinator who is supported in the role by the Network Manager and Computing subject leader to:

- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- provide training and advice for staff;
- liaise with the Local Authority/relevant body;
- liaise with school Network Manager and technical staff;
- review reports of online safety incidents on CPOMs to inform future online safety developments;
- meet regularly with Online safety Governor to discuss current issues, review incidents and filtering / change control logs;

- attend relevant meeting / committee of Governors;
- report regularly to the Senior Leadership Team.

Network Manager / Technical staff:

It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff. The managed service provider is fully aware of the school's online safety policy and procedures.

The Network Manager / ICT Technicians / Computing subject leader /Online safety Coordinator are responsible for ensuring:

- **that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;**
- **that the school meets the online safety technical requirements outlined in the Acceptable User Policy and any relevant Local Authority Online safety policy and guidance;**
- **that users may only access the school's network and devices through a properly enforced password protection policy, in which passwords are reviewed regularly and changed when appropriate;**
- the school's filtering policy is applied and updated on a regular basis;
- that the Network Manager keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant; that the use of the network / internet/ Learning Platform/ remote access / email addresses provided by the school are regularly monitored in order that any misuse / attempted misuse can be reported to the Online safety Co-ordinator /Headteacher / Senior Leader / Computing subject leader / Year leader for investigation / action / sanction as appropriate;
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

School Staff are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current school online safety policy and practices;**
- **they have read, understood and signed the school Staff Acceptable User Policy / Agreement (AUP);**
- **they report any suspected misuse or problem to the Online safety Co-ordinator /Headteacher / Senior Leader / Computing subject leader / Year Leader for investigation / action / sanction;**
- **all digital communications with pupils/ parents/ carers (email / Learning Platform should be on a professional level and only carried out using official school systems};**
- online safety issues are embedded in all aspects of the curriculum and other school activities;
- pupils understand and follow the school online safety and acceptable user policy (AUP);
- pupils have a good understanding of research skills and where appropriate the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons, extra-curricular and extended school activities 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.

Child protection & safeguarding commitment

The designated person/persons for child protection & safeguarding should be trained in online 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;
- Online bullying.

Online Safety Governor

The Online safety Governor will assist the Online safety Coordinator with:

- the production / review / monitoring of the school online safety policy / documents;
- the production / review / monitoring of the school filtering policy;
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/ carers and the pupils about the online safety provision
- monitoring improvement actions

Pupils:

- **are responsible for using school digital technology systems, in accordance with the Pupil Acceptable User Policy; they will be expected to sign the AUP before being given access to school systems;**
- have a good understanding of research skills and where appropriate 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 mobile devices. They should also know and understand school policies on the taking / use of images and on online bullying;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/ Carers/ Grandparents/ Relatives:

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 therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to sections of the website/ Learning Platform in accordance with the relevant school Acceptable User Policy.

Community Users:

Community users who access school systems/ website/ Learning Platform as part of the wider school provision will be expected to sign a Community User AUP (Acceptable User Policy) before being provided with access to school systems.

Policy Statements:

Education - pupils

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

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

- A planned online safety curriculum will be provided as part of the Computing, PHSE and National Curriculum. This should be regularly revisited to review the use of Computing and new technologies in school and outside school;
- Key online safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities;

- Pupils will 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 will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of Computing, the internet and mobile devices both within and outside school;
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use if pre-planned, pupils will 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 will be vigilant in monitoring the content of websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff confirm the authorisation of the Online Safety Co-ordinator to temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need – Authorisation RM Safety Net facilitates this.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of their children's on-line experiences/behaviours. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform;
- Parents evenings/workshops;
- High profile events/ campaigns e.g. Safer Internet Day, parent workshops
- Reference to appropriate Safe websites (nb the SWGfL "Golden Rules" for parents)

Education - Extended Schools

The school will offer advice and support to parents on online safety so that parents and children can work together to gain a better understanding of these issues. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff/Volunteers

It is essential that all staff, including volunteers with access to the internet receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly;
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable User Policies;
- The Online safety Coordinator (or other nominated persons) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by the LA and others;
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days;
- The Online safety Coordinator (or other nominated persons) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in Computing / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor hub CPD) / National Governors Association 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 / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable User Policy and any relevant Local Authority Online safety policy and guidance;
- 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;
- **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, by the Online safety Co-ordinator;
- **All users will be provided with a username and secure password** by the Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly.
- **The "master / administrator" passwords for the school technical system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe). The Network Manager will reset passwords when a member of staff leaves the school;**
- Staff will be responsible for the security of their username and password; they must not allow other users to access the systems using their log on details without their permission and must immediately report any suspicion or evidence that there has been a breach of security;
- The school maintains and supports the managed filtering service supported by Luton ICT Technical Service;
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader);
- Any filtering issues should be reported immediately to the Luton ICT Technical Service;
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Online safety Co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online safety Committee;
- 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 User Policy;
- Remote management tools are used by technical staff to control workstations and view users activity;
- An appropriate system is in place for technical staff, as agreed in the AUP to report any actual / potential online safety incident to the Network Manager or Online safety Co-ordinator;
- 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;
- 'Guests' may have temporary access to the school network via a generic password and will agree to abide by the AUP;
- An agreed policy is in place regarding the downloading of executable (.exe) files by users. Staff have agreed to check with the Network Manager/Technician before downloading executable files as detailed in the AUP;

- An agreed policy is in place regarding the extent of personal use that users (staff / pupils and their family members) are allowed on laptops and other portable devices that may be used out of school as detailed in the AUP;
- Staff have agreed to check with the Network Manager/Technician before installing programmes on school work stations/portable devices;
- Staff have agreed to follow the advice in the AUP with regards to the use of removable media devices;
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and multimedia images - Photographic, Video

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

- **When using digital images, staff should inform and educate students / 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;**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are reminded that any images of children taken at school events is for their own personal use. 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 any images.
- Staff are allowed to take digital / multimedia images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images;
- Care should be taken when taking digital / multimedia 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 use, share, publish or distribute images of others without the pupils and their parents permission;
- Photographs and multimedia images 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 or multimedia images;
- Written permission from parents or carers is obtained regarding the safe use of photographic and multimedia images published on the school website.
- Images taken on personal devices will follow school policies and procedures as outlined in the Acceptable User Policy.
- Photographs and multimedia images of children and staff will be kept on a secure server for a maximum of 3 years after they have left the school. Photographs used for display will be shredded after use.

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:

- **at all times they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;**
- **they 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;**
- **they transfer data using encryption and secure password protected devices.**

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

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

In line with General Data Protection Regulation (GDPR) and the Data Protection Act 2018, we hold pupil information while they attend St Joseph's Catholic Primary School. We may also keep it beyond their attendance if this is necessary in order to comply with our legal obligations. Please refer to the Privacy Notice, which is available on the school website.

In order to support pupils who have reported incidents of Online Safety, we record incidents on CPOMs and routinely share this information with Governors, Ofsted and external professionals. We do not share information about our children with anyone without consent unless the law and our policies allow us to do so.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				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 or multimedia images on mobile phones or other camera devices		√					√	
Use of mobile devices eg PDAs, PSPs	√						√	
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails				√				√
Use of chat rooms / facilities				√				√
Use of instant messaging – use of skype for planned curriculum		√					√	
Use of social networking sites				√				√
Use of blogs			√				√	

When using communication technologies the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored.** Staff should therefore only use the school email service to communicate with others when in school, or on school systems (e.g. by remote access). Pupils will use a messaging system within the Learning Platform;
- **Users need to be aware that email/message communications may be monitored;**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email/messages that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;**
- **Any digital communication between staff and pupils or parents / carers (email, chat, Learning Platform messages) 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. This includes the use of social networking sites to communicate with members of the school community on staff/pupils own personal devices. Staff should never communicate with pupils or parents using these sites and never with other staff for any school related issues. Any member of staff related to another member of the school community should never use a social networking site to communicate anything relating to school;
- Pupils will be provided with individual school email addresses for educational use. Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and 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	Acceptable for identified	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**					**X**
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					**X**
	adult material that potentially breaches the Obscene Publications Act in the UK					**X**
	criminally racist material in UK					**X**
	pornography				**X**	
	promotion of any kind of discrimination				**X**	
	promotion of racial or religious hatred				**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**	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LBC and / or the school					**X**	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					**X**	
Revealing or publicising confidential or proprietary information (e.g .financial / personal information, databases, computer / network access codes and passwords)					**X**	
Creating or propagating computer viruses or other harmful files					**X**	
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					**X**	
On-line gaming (educational) e.g. cool maths, education city live			**X**			
On-line gaming (non educational)					**X**	
On-line gambling					**X**	
On-line shopping / commerce			**X**			
File sharing		**X**				
School Use of social networking sites					**X**	
Home use of social networking sites		**X**				
Use of video uploading e.g. Youtube					**X**	
Use of school broadcasting for viewing only e.g. Youtube		**X**				

Responding to incidents of misuse

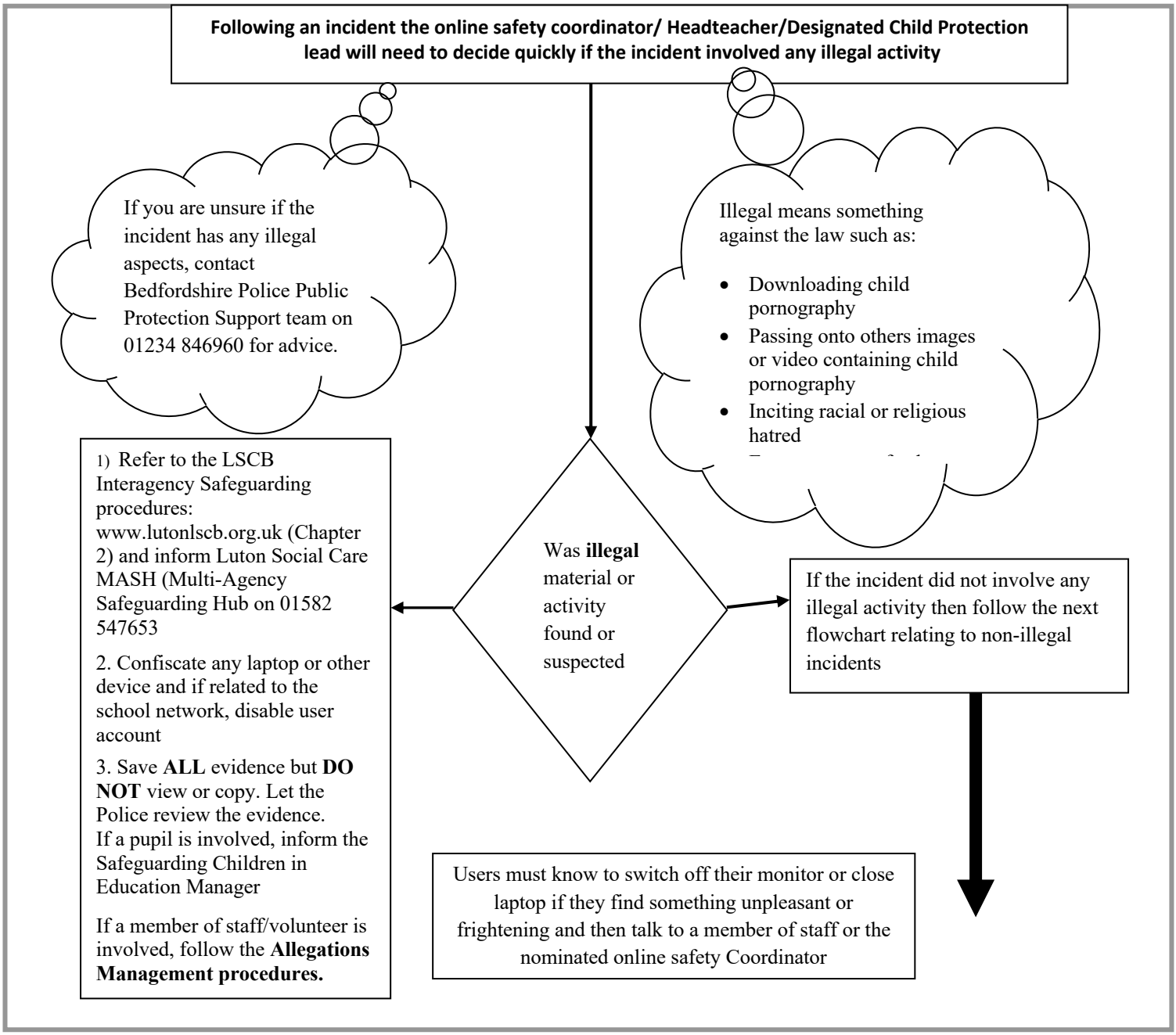
It is hoped that all members of the school community will be responsible users, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses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

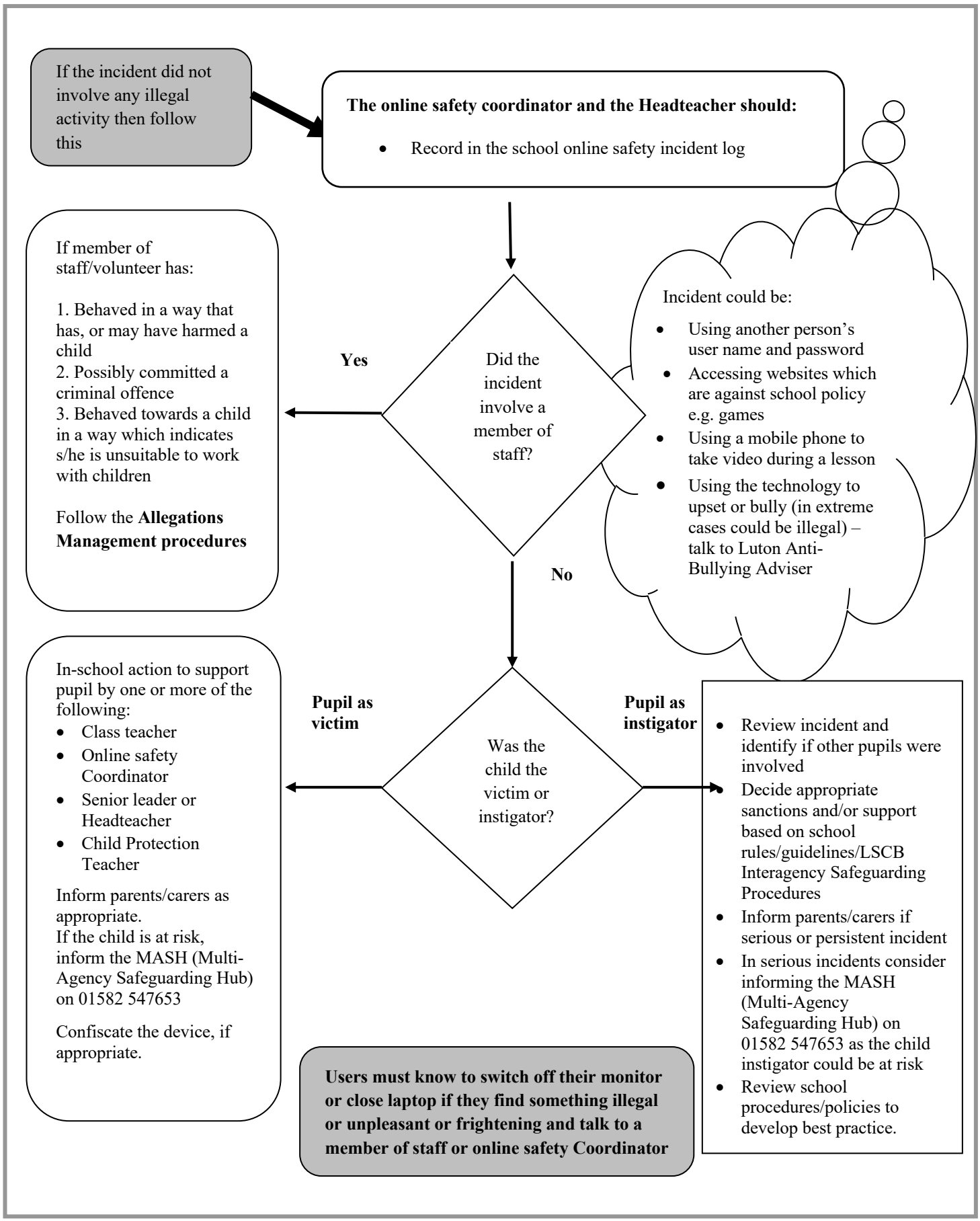
- **child sexual abuse images;**
- **adult material which potentially breaches the Obscene Publications Act;**
- **criminally racist material;**
- **other criminal conduct, activity or materials;**

the flow chart – below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Luton Flowchart to support decisions related to an illegal online safety incident



Luton Flowchart to support decisions related to non-illegal online safety incident



Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Year Leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	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).	X	X	X	X					
Unauthorised use of non-educational sites during lessons	X	X	X			X		X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X			X		X	X
Unauthorised use of social networking / instant messaging / personal email	X	X	X			X	X	X	X
Unauthorised downloading or uploading of files	X	X	X			X	X	X	X
Allowing others to access school network by sharing username and passwords	X	X	X			X	X	X	X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X			X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X	X	X	X
Corrupting or destroying the data of other users	X	X	X			X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Staff Actions / Sanctions

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

Legislation

Schools should be aware of the legislative framework under which this Online 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.

Glossary of terms

AUP	Acceptable User Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
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.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1 ..	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to 14)
LA	Local Authority
LAN	Local Area Network
Learning	A learning platform brings together hardware, software and supporting services
Platform	to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
SEF	Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark

SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
Learning Platform	Learning Platform (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

Online Safety Acceptable User Policy
Staff COPY

In the Light of Jesus we Learn to Shine

Member of staff: .....

School Policy

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 to support effective learning. All users have an entitlement to safe internet access at all times.

The school will try to ensure that staff will have good access to technology to enhance their teaching and pupils' learning and will, in return, expect the staff to agree to be responsible users.

This Acceptable User Policy is intended to ensure that:

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

This policy must be read in conjunction with the school's Online Safety Policy. By signing this Acceptable User Policy you are stating that you have also read the Online Safety Policy and agree to abide by all the terms and guidelines within both policies.

If a member of staff is not willing to sign the Acceptable User Policy, so indicating that they do not accept the terms within this and the Online Safety Policy, then he/she will not be able to use any of the school's ICT devices nor access any of the school's on-line facilities.

Acceptable User Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the computing systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school computing systems (e.g. laptops, email, Learning Platform etc) out of school;
- I understand that the school computing 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 except in exceptional circumstances. Nor will I try to use any other person's username and password without their express permission. A central record of individual passwords will be kept by the Network Manager;
- 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 computing 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 / multimedia images;
- If I choose to use my personal equipment to record images during the school day or on schools trips I will download them to school equipment as soon as feasibly possible. I will remove all images from the equipment once downloaded. Where these images are published (e.g. on the school website, Learning Platform) 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 outside of school for personal use and will never communicate anything relating to school community – see Online Safety Policy;
- 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 – refer to the **Online Safety Policy** for further guidance.

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

- When I use my personal devices (mobile devices/ 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 (refer to the **Online Safety Policy** for further guidance);
- I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses;
- I will ensure that my data on external storage devices 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 outside or within teaching hours to avoid taking 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, unless this is allowed in school policies. Before downloading any software, either for school or personal use, I will liaise with the Network Manager.
- 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 LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted;
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority;
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not download or distribute copies (including music and multimedia images).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable User Policy applies not only to my work and use of school computing equipment in school, but also applies to my use of school computing systems and equipment out of school and my use of personal equipment in school or in situations (including outside of school) related to my employment by the school;
- I understand that if I fail to comply with this Acceptable User Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

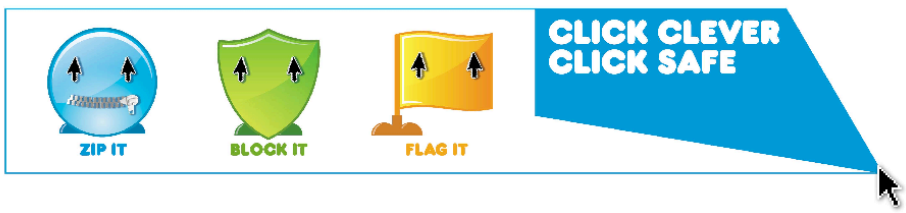
I have read and understand the terms and guidelines set out in the Acceptable User Policy for staff and in the school's Online Safety Policy. I agree to use the school's Computing systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) as detailed in these terms and guidelines. I also agree to the terms and guidelines relating to the use of services and sites accessed through the internet (both on the school's or my own personal computing equipment) in order to communicate with, or in relation to, members of the school community.

Name: .....

Signature: .....

Date: .....

PLEASE SIGN AND RETAIN THIS POLICY.



Staff COPY

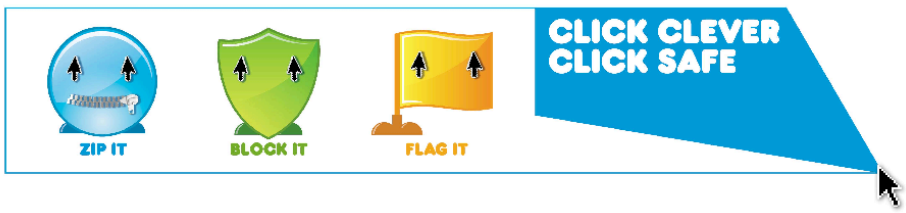
I have read and understand the terms and guidelines set out in the Acceptable User Policy for staff and in the school's Online Safety Policy. I agree to use the school's computing systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) as detailed in these terms and guidelines. I also agree to the terms and guidelines relating to the use of services and sites accessed through the internet (both on the school's or my own personal computing equipment) in order to communicate with, or in relation to, members of the school community.

Name: .....

Signature: .....

Date: .....

PLEASE SIGN AND RETURN THIS SHEET TO THE SCHOOL OFFICE.



In the Light of Jesus we Learn to Shine

Online Safety Acceptable User Policy
SCHOOL COPY
Parent/Carer of pupils in Early Years

Name of Pupil: ..... **Class: .....**

THIS COPY TO BE SIGNED BY PUPIL AND PARENT AND RETURNED TO SCHOOL.

When I am using the computer or other technologies (see list below for examples), I want to feel safe all the time.

I will not bring into school any of the following devices without permission:

- ☹ Mobile Devices, including laptops, iPads, tablets, netbooks, ebook readers
- ☹ Camera including still and video cameras, Webcam
- ☹ Gaming Devices including Nintendo 3DS, Sony Playstations, The MG Portable Android Gaming System

I agree that I will:

- always keep my password a secret;
- talk to my teacher before using anything new on the internet;
- ask permission before signing up to any websites and always use my learning platform email address to do so;
- tell my teacher if anything makes me feel scared or uncomfortable;
- make sure all messages/postings I send or write are polite;
- show my teacher if I receive an unkind message;
- not reply to any message or anything which makes me feel uncomfortable;
- never give my mobile phone number to anyone on the internet;
- only email or message people I know;
- I will only use my school email address, when I am at school;
- I will not tell people about myself online (I will not tell them my name, anything about my home and family and pets);
- I will not load photographs of myself onto the computer, without the permission of my parents/carer;
- I will not upload images of others onto the internet without the express permission of those pupils and their parents;
- never agree to meet a stranger.

I understand that anything I do on the computer may be seen by someone else. I agree to be a responsible user and stay safe while using the internet and other communications technologies, both in and out of school.

Parents/Carers

Your child will develop a growing awareness of Computing as they progress through the school curriculum. We ask parents to support us in the Online Safety Policy and use of technologies **at an age appropriate level**.

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

I understand that my child's activity on the computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable User Policy.

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

I have read this Online Safety Acceptable User Policy and have discussed it with my child.

I agree/do not agree (delete as appropriate) to support the school's policy on online safety.

Please be aware that if you do not sign the agreement to support the school's policy on online safety, your child will be unable to use computing equipment, or to have access to the internet, in school.

Signed: (Parent/Carer) ……..…….....

Date: ..... / ..... / .....

In the Light of Jesus we Learn to Shine

Online Safety Acceptable User Policy
SCHOOL COPY
Parent/Carer of pupils in KS1

Name of Pupil: ..... **Class: .....**

THIS COPY TO BE SIGNED BY PUPIL AND PARENT AND RETURNED TO SCHOOL.

When I am using the computer or other technologies (see list below for examples), I want to feel safe all the time.

I will not bring into school any of the following devices without permission:

- ☹ Mobile Devices, including laptops, iPads, tablets, netbooks, ebook readers
- ☹ Camera including still and video cameras, Webcam
- ☹ Gaming Devices including Nintendo 3DS, Sony Playstations, The MG Portable Android Gaming System

I agree that I will:

- always keep my password a secret;
- talk to my teacher before using anything new on the internet;
- ask permission before signing up to any websites and always use my learning platform email address to do so;
- tell my teacher if anything makes me feel scared or uncomfortable;
- make sure all messages/postings I send or write are polite;
- show my teacher if I receive an unkind message;
- not reply to any message or anything which makes me feel uncomfortable;
- never give my mobile phone number to anyone on the internet;
- only email or message people I know;
- I will only use my school email address, when I am at school;
- I will not tell people about myself online (I will not tell them my name, anything about my home and family and pets);
- I will not load photographs of myself onto the computer, without the permission of my parents/carer;
- I will not upload images of others onto the internet without the express permission of those pupils and their parents;
- never agree to meet a stranger.

I understand that anything I do on the computer may be seen by someone else. I agree to be a responsible user and stay safe while using the internet and other communications technologies, both in and out of school.

Pupil signature: _____ Date: _____

Parents/Carers

Your child will develop a growing awareness of Computing as they progress through the school curriculum. We ask parents to support us in the Online Safety Policy and use of technologies **at an age appropriate level**.

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

I understand that my child's activity on the computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable User Policy.

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

I have read this Online safety Acceptable User Policy and have discussed it with my child.

I agree/do not agree (delete as appropriate) to support the school's policy on online safety.

Please be aware that if you do not sign the agreement to support the school's policy on online safety, your child will be unable to use computing equipment, or to have access to the internet, in school.

Signed: (Parent/Carer) ……..…….....

Date: ..... / ..... / .....

In the Light of Jesus we Learn to Shine

Online Safety Acceptable User Policy

SCHOOL COPY

Yr 3 & Yr 4 Pupils

Name of Pupil: ..... **Class: .....**

THIS COPY TO BE SIGNED BY PUPIL AND PARENT AND RETURNED TO SCHOOL.

When I am using the computer or other technologies (see list below for examples), I want to feel safe all the time.

I will not bring into school any of the following devices:

- ☹ Mobile phones, including Smart Phones, Blackberries, iPhones
- ☹ Mobile Devices, including laptops, iPads, tablets, netbooks, ebook readers
- ☹ Camera including still and video cameras, Webcam
- ☹ Gaming Devices including Nintendo 3DS, Sony Playstations, and Portable Android Gaming System

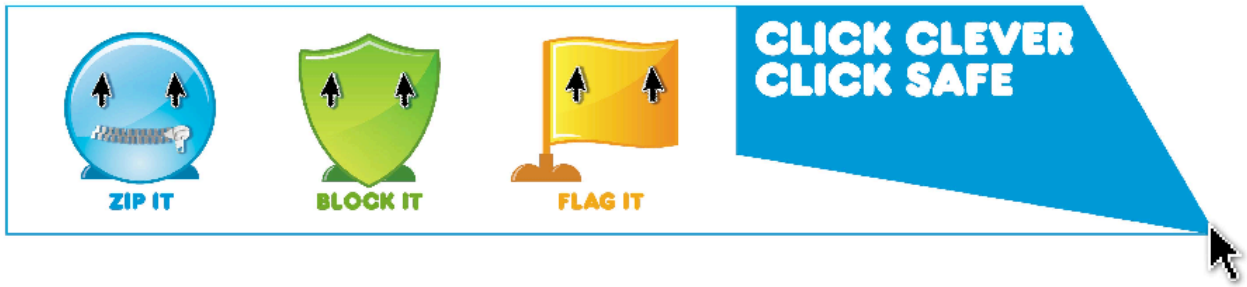
*I will only bring in a camera or hand held device with permission from my parents and the school. I will use these devices responsibly and in line with school policy.

I agree that I will:

- always keep my password a secret;
- talk to my teacher before using anything new on the internet;
- ask permission before signing up to any websites and always use my learning platform email address to do so;
- tell my teacher if anything makes me feel scared or uncomfortable;
- make sure all messages/postings I send or write are polite;
- show my teacher if I receive an unpleasant message;
- not reply to any message or anything which makes me feel uncomfortable;
- never give my mobile phone number to anyone on the internet;
- only email or message people I know;
- I will only use my school email address, when I am at school;
- I will not tell people about myself online (I will not tell them my name, anything about my home and family and pets);
- I will not load photographs of myself onto the computer, without the permission of my parents/carer;
- I will not upload images of others onto the internet without the express permission of those pupils and their parents.
- never agree to meet a stranger.
- I understand that when using social media sites or any form of communication tool I follow the terms and conditions of those sites appropriately.

I understand that anything I do on the computer may be seen by someone else. I agree to be a responsible user and stay safe while using the internet and other communications technologies, both in and out of school.

Pupil signature: _____ Date: _____



Parents/Carers

Your child will develop a growing awareness of Computing as they progress through the school curriculum. We ask parents to support us in the Online Safety Policy and use of technologies **at an age appropriate level.**

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

I understand that my child's activity on the computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable User Policy.

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

I have read this Online safety Acceptable User Policy and have discussed it with my child.

I agree/do not agree (delete as appropriate) to support the school's policy on online safety.

Please be aware that if you do not sign the agreement to support the school's policy on online safety, your child will be unable to use computing equipment, or to have access to the internet, in school.

Signed: (Parent/Carer) ……..…….....

Date: ..... / ..... / .....

In the Light of Jesus we Learn to Shine

Online Safety Acceptable User Policy
SCHOOL COPY
Yr 5 & Yr 6 Pupils

Name of Pupil: ..... **Class: .....**

THIS COPY TO BE SIGNED BY PUPIL AND PARENT AND RETURNED TO SCHOOL.

When I am using the computer or other technologies (see list below for examples), I want to feel safe all the time.

I will not bring into school any of the following devices:

- ☹ Mobile phones, including Smart Phones, Blackberries, iPhones
- ☹ Mobile Devices, including laptops, iPads, tablets, netbooks, ebook readers
- ☹ Camera including still and video cameras, Webcam
- ☹ Gaming Devices including Nintendo 3DS, Sony Playstations and Portable Android Gaming System

I will use these devices responsibly and in line with school policy.

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

For my own personal safety:

- I understand that the school will monitor my use of the computing systems, email and other digital communications;
- I will keep my username and password secure – I will not share it, nor will I try to use any other person's username and password;
- I will be aware of "stranger danger", when I am communicating on-line;
- I will not disclose or share personal information about myself or others when on-line;
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school computing systems are intended for educational use.

I will act as I expect others to act towards me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will not upload images of others onto the internet without the express permission of those pupils and their parents.

I recognise that the school has a responsibility to maintain security to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others;
- I will immediately report any damage or faults involving equipment or software, however this may have happened;
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes;

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, not will I try to alter computer settings.

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

- I should ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not try to download copies (including music and multimedia images);
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that when using social media sites or any form of communication tool I follow the terms and conditions of those sites appropriately.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour towards any member of the school community when I am out of school (examples would be online bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable User Policy Agreement, the school will take action in line with the School Behaviour Policy. This may also include loss of access to the school network / internet, contact with parents/carers and in the event of illegal activities involvement of the police.

I have read and understand the above and agree to be a responsible user and stay safe while using the internet and other communications technologies, both in and out of school, for learning, personal and recreational use.

Pupil signature: ..... Date: .... / .... / .....

Parents/Carers

Your child will develop a growing awareness of Computing as they progress through the school curriculum. We ask parents to support us in the Online Safety Policy and use of technologies **at an age appropriate level.**

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

I understand that my child's activity on the computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable User Policy.

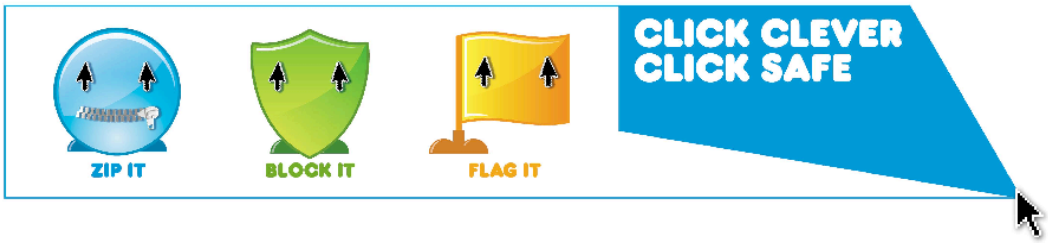
I will encourage my child to adopt **age appropriate** safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

I have read this Online safety Acceptable User Policy and have discussed it with my child.

I agree/do not agree (delete as appropriate) to support the school's policy on online safety.

Please be aware that if you do not sign the agreement to support the school's policy on online safety, your child will be unable to use computing equipment, or to have access to the internet, in school.

Signed: (Parent/Carer) ……..……..... Date: ……/ ……/ …….



Use of Digital / Multimedia Images

The use of digital / multimedia images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,
The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above pupil, I agree to the school taking and using digital / multimedia images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or multimedia images at, or of, school events, which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed		Date	

Online Safety – A School Charter for Action

In the Light of Jesus we Learn to Shine

Name of School	St Joseph's Catholic Primary School
Name of Local Authority	Luton

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential online safety risks.

Our school community
Discusses, monitors and reviews our Online Safety Policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports **staff** in the use of Computing as an essential tool for enhancing learning and in the embedding of online safety across the whole school curriculum.

Ensures that **pupils** are aware, through online safety education, of the potential online safety risks associated with the use of computing and mobile technologies, that all online safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's Online Safety Policy.

Provides opportunities for **parents/carers** to receive online safety education and information, to enable them to support their children in developing good online safety behaviour. The school will report back to parents / carers regarding online safety concerns. Parents/carers in turn work with the school to uphold the Online Safety Policy.

Seeks to learn from online safety good practice elsewhere and utilises the support of the **LA and relevant organisations** when appropriate.

Chair of Governors	
Headteacher	
Online Safety Co-ordinator	
Online Safety Governor	
Pupil Representative	
Parent Representative	

In the Light of Jesus we Learn to Shine

Online Safety Acceptable User Policy
School COPY
School Guests/Visitors

Name of guest/visitor: .....

School Policy

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 to support effective learning. All users have an entitlement to safe internet access at all times.

If applicable the school will try to ensure that guests/visitors will have good access to technology to enhance teaching and learning and will in return expect the guest/visitor to agree to be responsible users.

This Acceptable User Policy is intended to ensure that:

- All school guests/visitors will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- School computing systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- All technology users are protected from potential risk in their use of technology in their everyday work.

This policy must be read in conjunction with the school's Online Safety Policy. By signing this Acceptable User Policy you are stating that you have also read the Online Safety Policy and agree to abide by all the terms and guidelines within both policies.

If a guest/visitor is not willing to sign the Acceptable User Policy, so indicating that they do not accept the terms within this and the Online Safety Policy, then he/she will not be able to use any of the school's ICT devices nor access any of the school's on-line facilities.

Acceptable User Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the computing systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school computing systems (e.g. laptops, email, Learning Platform etc) out of school; (*if applicable*)
- I understand that the school computing 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 given username or password to anyone else except in exceptional circumstances. Nor will I try to use any other person's username and password without their express permission. A central record of individual passwords will be kept by the Network Manager;

- 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 computing 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;
- If I choose to use my personal equipment to record images during the school day or on schools trips I will download them to school equipment as soon as feasibly possible. I will remove all images from the equipment once downloaded. Where these images are published (eg on the school website, Learning Platform) it will not be possible to identify by name, or other personal information, those who are featured; *(if applicable*)
- I will only use chat and social networking sites outside of school for personal use and will never communicate anything relating to school community – see Online Safety Policy;
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner; (*if applicable*)
- I will not engage in any on-line activity that may compromise my professional responsibilities – refer to the **Online Safety Policy** for further guidance.

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

- When I use my personal devices (mobile devices / 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 (refer to the **Online Safety Policy** for further guidance);
- I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses;
- I will ensure that my data on external storage devices 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 outside or within teaching hours to avoid taking 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, unless this is allowed in school policies. Before downloading any software, either for school or personal use, I will liaise with the Network Manager.
- 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 LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted;
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority;
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not download or distribute copies (including music and multimedia images).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable User Policy applies not only to my work and use of school computing equipment in school, but also applies to my use of school computing systems and equipment out of school and my use of personal equipment in school or in situations (including outside of school) related to my work within the school;
- I understand that if I fail to comply with this Acceptable User Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

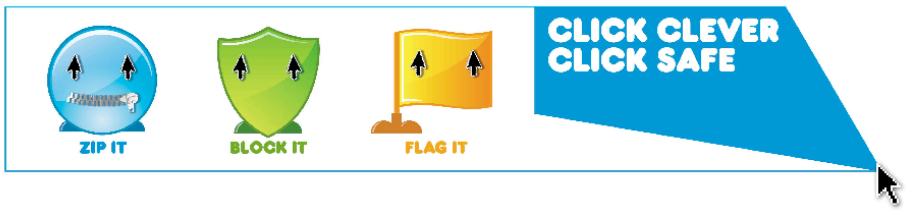
I have read and understand the terms and guidelines set out in the Acceptable User Policy for school guests/visitors and in the school's Online Safety Policy. I agree to use the school's computing systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) as detailed in these terms and guidelines. I also agree to the terms and guidelines relating to the use of services and sites accessed through the internet (both on the school's or my own personal computing equipment) in order to communicate with, or in relation to, members of the school community.

Name: .....

Signature: .....

Date: .....

PLEASE SIGN AND RETAIN THIS POLICY.



In the Light of Jesus we Learn to Shine

Online Safety Acceptable User Policy

School Copy

School guests/visitors

I have read and understand the terms and guidelines set out in the Acceptable User Policy for staff and in the school's Online Safety Policy. I agree to use the school's computing systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) as detailed in these terms and guidelines. I also agree to the terms and guidelines relating to the use of services and sites accessed through the internet (both on the school's or my own personal computing equipment) in order to communicate with, or in relation to, members of the school community.

Name: .....

Signature: .....

Date: .....

PLEASE SIGN AND RETURN THIS SHEET TO THE SCHOOL OFFICE.