ICT Safety and Acceptable Use Policy

St Mary's Catholic Primary School

Ratified by Governors: October 2020

Safeguarding, Health and Safety (incl. Premises) sub-committee

Review Date: October 2021

Approved by:	Safeguarding Health and Safety Governor's Sub-Committee	**Date:** 13.10.20
Last reviewed on:	13.10.20	
Next review due by:	30.10.21	

Written by: C. McManus

Table of Contents

Heading	Page
Roles	3
Development, Monitoring and Review of this Policy	3
Schedule for development, monitoring and review	3
Scope of the Policy	4
Roles and Responsibilities	4
Governors	4
Headteacher and Senior Leaders	5
E-safety Lead	5
Network Support Team / IT Technician	5
Teaching and Support Staff	6
Designated Safeguarding Leads (DSLs)	6
E-safety Working Group	6
Pupils	7
Parents and Carers	7
Community Users	8
Policy Statements	8
Education – pupils	8
Education – parents and carers	8
Education – The Wider Community	9
Education & Training – Staff / Volunteers	9
Training – Governors	9
Technical – infrastructure, equipment, filtering and monitoring	10
Protection from harm	11
Reporting concerns	11
Digital Images and Video	11
Data Protection	12
Communications	13
Prevent Duty	15
Social Media - Protecting Professional Identity	15
Unsuitable / inappropriate activities	16
Responding to incidents of misuse	17
Illegal Incidents	17
Other Incidents	17
Flowchart for responding to incidents	18
Dealing with Incidence of Misuse	19
Appendix	21
Acknowledgements	21

Roles

Role	Name	Onsite/ Offsite
Headteacher	Claire McManus	Onsite
E-safety lead	Claire McManus	Onsite
IT Lead	C/O Claire McManus	Onsite
Safeguarding governor	Samantha Foster	School Affiliate Onsite
IT technician	Remedian IT Specialist	Weekly ½ day visit by Ben McLeish
Network support team	Remedian IT Specialist	Remote/ Offsite
Designated Safeguarding Leads (DSLs)	Claire McManus Jan Robinson Emma Chorley	Onsite

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by a working group made up of:

- Headteacher and Senior Leaders
- E-Safety Officer
- Staff – including Teachers, Support Staff, Technical staff
- Governors

Schedule for development, monitoring and review

This e-safety policy was approved by the Governing Body	September 2017
The implementation of this e-safety policy will be monitored by the:	E-safety lead Senior Leadership Team Safeguarding Governor
Monitoring will take place at regular intervals:	Every June
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Every June
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	Every June
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager LA Safeguarding Officer Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Automatic monitoring of logs of internet activity (including sites visited). These automatically forward concerns and inappropriate use to safeguarding staff.
- Automatic monitoring of computer network activity.
- Surveys / questionnaires of (every June)
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

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 e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

The 'After School Provision': Bees Knees, will follow and adhere to all aspects of this policy, monitoring usage, keeping children safe, reporting any misuse as well as keeping e-safety at the forefront of all internet activities.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing *Body* has taken on the role of Safeguarding Governor and e-safety will be overseen as part of this role. Safeguarding Governor termly meetings with the Head on safeguarding will also include:

    - E-safety update
    - Termly report of e-safety incidents
    - Termly report on changes to filtering
- Reporting at relevant Governors meetings on safeguarding by the Safeguarding Governor will include above information on e-safety

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e- Safety Officer.
- The Headteacher and Deputies will 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).
- The Headteacher is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive termly monitoring reports from the E-Safety Officer.

E-safety Lead

- Leads the e-safety group
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Meets termly with Safeguarding Governor and Head to discuss current issues, review incident logs and filtering-change control logs
- Attends relevant meeting of Governors
- Reports regularly to Senior Leadership Team
- Ensures that e-safety issues raised are documented, followed up and resolved in-line with policy and procedure

Network Support Team / IT Technician

The Technical staff are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements and any Local Authority E-Safety Policy that may apply. (At present, there isn't one.)
- That users may only access the networks and devices through a properly enforced password protection policy, Passwords should be hard to guess, contain at least one number and both upper and lowercase letters and they should not be a single word. It is recommended that users use a phrase to make remembering their passwords easier. Passwords should be changed at the beginning of each school year.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. (see below: *Technical – infrastructure, equipment, filtering and monitoring*.).

- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network, internet, remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and E-Safety Officer for investigation.
- That monitoring software and systems (Impero) are implemented and updated as set out in this policy

Teaching and Support Staff

are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and procedures
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problems to the Headteacher or E-safety Lead for investigation
- All digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems (see appendix)
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use policies (see appendix)
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that children and staff understand what they need to do if unsuitable material is found in internet searches.

Designated Safeguarding Leads (DSLs)

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

E-safety Working Group

The E-safety Working Group is a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring of the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Working Group will assist the E-Safety Officer and other relevant persons, as above, with:

- The production, review and monitoring of the school e-safety policy and documents.
- The production, review and 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 and incident logs
- Consulting stakeholders – including parents / carers and the pupils about the e-safety provision

(Note: An E-Safety Working Group Terms of Reference Template can be found in the appendices)

Pupils

- Are responsible for using the school digital technology systems in accordance with the (age appropriate) Pupil Acceptable Use Agreement (AUA).
- Are responsible for gaining 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 to know how to do so:
    - Turn off screen
    - Report to responsible adult
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking of images, on the use of these images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school, as covered by the curriculum.
- Need to realise that the school's AUA covers their actions out of school, if related to their membership of the school.
- When out of school, if accessing something that has been set up within school, such as email accounts, google classroom etc., school e-safety policies apply, the curriculum content must be followed and AUA applies to their actions.

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national and local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line pupil records

Community Users

Community Users who access school systems and the school website as part of the wider school provision will be expected to sign a Community User AUA 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of Computing, PHSE and other lessons and should be regularly revisited in lessons for every age group.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities (see appendix)
- Pupils should be 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Any such temporary access needs to use a timed 'window of access' so that the filtering automatically begins to filter the website again after the session completes. In addition, the filter must be checked to ensure that the protection is re-established, and this must be marked as such on the filtering change request log.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit by ensuring that screens of the children are visible to the managing staff, through good teaching practice, reminding children of their responsibility for whistle blowing on inappropriate or unsafe behaviour, and through the use of remote screen monitoring.

Education – Parents and Carers

Many parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- 'Parent/Carer friendly' language on School website
- 'The school line' on e-safety issues of the day - on School website
- Parent Hub notifications
- Parents and Carers evenings
- High profile events and campaigns e.g. Safer Internet Day
- Reference to the relevant websites and publications

Education – The Wider Community

The school will provide opportunities for the local community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards other relatives as well as parents/carers.
- The school website will provide e-safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be updated yearly in July and developed to meet the changing needs of e-safety. An audit of the e- safety training needs of all staff will be carried out as part of this work. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The e-Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations. Learning outcomes are shared with staff and published on the website where appropriate.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.

Training – Governors

Governors should take part in e-safety training and awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training and information sessions for staff or parents. This may include attendance at assemblies and lessons.
- Participation in E-Safety Working Group.

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 need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be October 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.
- All users at KS2 and above (including children) will be provided with a username and secure password by the school technician who will retain access to user accounts so that password can be changed and accounts retrieved. Users are responsible for the security of their username and password and will be required to change their password at the beginning of the year. School chooses to use group or class logons and passwords for KS1 and below, but need to be aware of the risks of documents being moved, edited or accidently deleted.
- The "administrator" passwords for the school ICT system, used by the network support staff must also be available to the Headteacher or Deputies and kept in a secure place (eg school safe).
- The IT Lead is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (such as child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and automatically monitored.
- There is a clear process in place to deal with requests for filtering changes
- The school has provided differentiated user-level filtering, allowing for filtering for different age-groups and different user groups
- Automatic monitoring and recording of the activity of users on the school technical systems flags concerning activity and routed to DPs. Users are made aware that their activity is monitored in the Acceptable Use Agreement.
- An appropriate system is in place (see appendix) for users to report any actual or potential technical incident or security breach to the relevant person.
- Appropriate security measures are in place (see appendix) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (see appendix) for the provision of temporary access of 'guests' (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (see below) regarding the extent of personal use that users (staff, pupils and community users) and their family members are allowed on school devices that may be used out of school.
- Staff are not allowed to download executable files onto school technology, though they can request that IT support staff do this for them. Any software used by children should be risk assessed.
- An agreed policy is in place (see appendix) regarding the use of removable media (eg memory sticks, CDs and DVDs etc.) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Protection from harm

The internet provides children and young people with access to a wide-range of content, some of which is harmful. The range of harm covers the scope of material from inappropriate to extreme. Content is defined here as images, websites or parts of websites, advertising, videos, text or other material found on the web or accessed through the internet.

Inappropriate content is not suitable or proper in the circumstances for the user, (specifically taken in this policy to mean the users age.) Something that is appropriate for an older age group can be inappropriate for a younger age group.

Harmful content is content that is both inappropriate and harmful to the user. In the school context, we are here referring to content that is harmful to children. This harm includes emotional and psychological aspects. Cases which relate to physical harm are treated as illegal (see below).

Extremist content is not allowed and should be reported to the police. Extremism is the vocal or active opposition to our fundamental British values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. We also regard calls for the death of members of the UK armed forces as extremist.

Illegal content as defined in UK law is unacceptable for all users. Any instance of criminal illegal content should be reported to the police.

Reporting concerns

Children should immediately report any inappropriate, harmful, extremist or illegal content or behaviour to a supervising adult.

Adults any material or behaviour which an adult sees or finds that is inappropriate, harmful, extremist or illegal must be handled using the flowchart below: Flowchart for responding to incidents. As prescribed in the flowchart, they must also alert the e-safety lead and a designated safeguarding lead, and must fill in the relevant safeguarding and e-safety reporting sheets, and share them with these people.

E-safety Lead and DSLs are responsible for handling the incident in accordance with the incident response procedure.

Digital Images and Video

The development of digital cameras, video recorders, smartphones and other digital image capture devices have created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published nor made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used.
- 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. (For example, photos of children at a swimming gala would be considered inappropriate.)
- 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 by teachers and will comply with good practice guidance (only the first name of pupils should be used, there should be parent permission to use the image) on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

- Responsible persons are appointed - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office. Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- The use of removable media is not allowed for the storage of personal data unless it meets the above requirements.

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:

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. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the appropriate person (the class teacher for children, or the e-safety lead for adults) – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, Virtual Learning Environment (VLE) etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Communication Technology	Staff and Other Adults			Pupils		
	Allowed	Allowed with approval from SLT	Not allowed	Not allowed	Allowed	Allowed with staff permission
Mobile phones may be brought to school	X			X		
Use of mobile phones in lessons			X	X		
Use of mobile phones in social time	X			X		
Taking photos on mobile phones/cameras			X	X		
Use of other mobile devices e.g. tablets, gaming devices	X				X	
Use of personal email addresses in school, or on school network	X					X
Use of school email for personal emails		X		X		
Use of messaging apps	X			X		
Use of social media	X					X
Use of blogs	X				X	

Prevent Duty

Extremists can use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content.

We also filter out social media, such as Facebook. Searches and web addresses are monitored and concerns are forwarded to Safeguarding Designated Persons where there are concerns. IT staff will prevent further access when new sites that are unblocked are found. Where staff, students or visitors find unblocked harmful, extremist or illegal content they must report it to a senior member of staff.

The Acceptable Use Agreement (AUA) refers to preventing radicalisation and related extremist content. Pupils and staff are asked to sign the AUA annually to confirm they have understood what is acceptable.

The school has a comprehensive collection of procedures for handling e-safety concerns, logging, reporting and development. These can be found in the appendix. Staff know how to access these procedures and how to use them to handle e-safety concerns or incidents.

Pupils know how to report internet content that is inappropriate or of concern.

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 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, ethnicity or disability or who defame a third party, may render the school 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 minimize 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 pupils, parents / careers 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* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the Head to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

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

User Actions 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: This refers to **all users** except where otherwise stated.	Acceptable	Acceptable **for staff** on school business, outside of learning time	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
Pornography				X	
Promotion of any kind of discrimination				X	
Threatening behaviour, including promotion of physical violence or mental harm				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing	X				
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services (e.g. email, video sharing services, document collaboration). It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

- An investigation group will be formed with more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- The procedure will be conducted using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. The same computer will be used for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- The URL of any site containing the alleged misuse must be recorded and the nature of the content causing concern to be described. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of 'grooming' behaviour
    - The sending of obscene materials to a child
    - Adult material which potentially breaches the Obscene Publications Act
    - Criminally racist material
    - Other criminal conduct, activity or materials
- The computer in question must be isolated where possible. Any change to its state may hinder a later police investigation.

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

Illegal Incidents

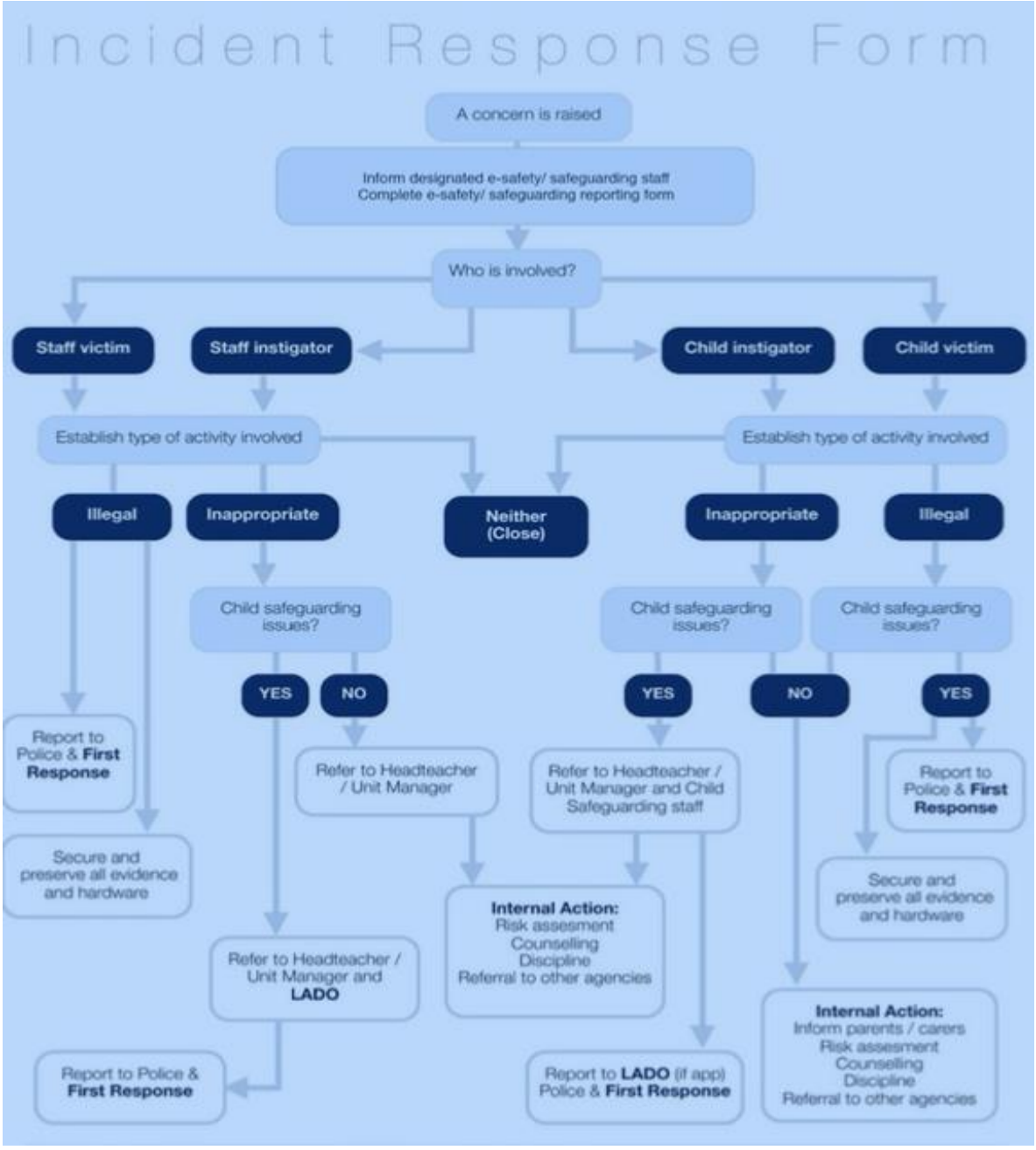
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In these cases, refer to the left-hand side of the Flowchart (below and appendix)

Flowchart for responding to incidents

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



Telephone numbers:
LADO: The Local Authority Designated Officer in Tameside: Tania Brown 0161 342 4398
Email: tania.brown@tameside.gov.uk Referrals are made to: ladoreferrals@tameside.gov.uk
When Tania Brown is not available contact the Independent reviewing duty Officer on 0161 342 4343.

First Response Team:
Monday to Friday during office hours Tel: 0161 342 4101
Monday to Friday outside office hours and weekends and public holidays Tel: 0161 342 2222

Dealing with Incidence of Misuse

Pupil Incidents	Refer to class teacher	Refer to Head of Phase/ Deputy	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 e.g. 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	X		
Unauthorised use of non-educational sites during lessons	X	X				X			
Unauthorised use of mobile phone / digital camera /other mobile device	X	X				X		X	
Unauthorised use of social media / messaging apps / personal email	X	X				X		X	
Unauthorised downloading or uploading of files	X	X				X		X	
Allowing others to access school network by sharing username and passwords	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	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X	X	X	
Corrupting or destroying the data of other users	X	X				X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions			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	
Using proxy sites or other means to subvert the school's filtering system		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	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X				X		X	
Incidents of 'sexting'			X			X			

Staff: Actions and Sanctions

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

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

Acknowledgements

St. Mary's Catholic Primary School would like to acknowledge the South West Grid for Learning as the originator of the template from which this policy was developed. www.swgfl.org.uk