Raysfield Primary

Know myself. Respond to my world.
Connect with my community.

E-SAFETY POLICY

Signed (Chair):	Name: David Champion	Date: 10th January 2021
Signed (Head):	Name: Claire Hill	Date: 10th January 2021
Ratified: by Standards Committee – 10th January 2021		Next Review: 2 years – January 2023

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices	E-Safety Policy	Date	10th January 2021
EIA CARRIED OUT BY:	Claire Hill	EIA APPROVED BY:	Standards Committee

Groups that may be affected:

Are there concerns that the policy could have a different impact on any of the following groups? (Please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for a positive impact
Age (young people, the elderly; issues surrounding protection and welfare, recruitment, training, pay, promotion)		✓
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication).		✓
Gender Reassignment (transsexual)		✓
Marriage and civil partnership		✓
Pregnancy and maternity		✓
Racial Groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers)		✓
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		✓
Gender (male, female)		✓
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		✓

Any adverse impacts are explored in a Full Impact assessment

We take opportunities to maximize positive impacts for sexuality, disabled and non-disabled people, people of different ethnic, cultural and religious backgrounds, girls, boys, men and women.

Links with other policies

This policy is linked with the following Raysfield policies:
Anti Bullying
Child Protection
Safeguarding
Acceptable Use – Staff
Acceptable Use – Pupils
Acceptable Use – Parents

Policy: Online E-Safety Policy

The Internet and other technologies have the potential to offer many positive benefits to young people. As with everything, this is not without risk. We want young people to be able to fully exploit the benefits offered by IT while doing so in a safe manner. Online messaging, social networking and mobile technology effectively mean that children can always be 'online'. Their social lives, and therefore their emotional development, are bound up in the use of these technologies.

The purpose of this policy is to ensure that the school community are kept aware of the risks as well as the benefits of technology and how to manage these risks and keep themselves and others safe. It details the measures that the school have put in place to support this.

E-safety Working Group

The e-safety policy has been developed with reference to the South Gloucestershire / Integra Schools guidance. It will be reviewed and monitored by our school online safety working group which comprises of:

- Headteacher
- School Online Safety coordinator / IT subject leader
- A parent governor representative
- PSHE leader

Consultation with the whole school takes place through staff meetings, governor meetings and parent meetings.

Monitoring and Review

Schedule for Development, Monitoring and Review

Policy ratified by the *Governing Body on::*	January 2021
The implementation of this policy will be monitored by:	E-safety working group
Monitoring will take place:	Annually during Term 6
The *Governing Body* will receive a report on the implementation including reported incidents:	Annually during Term 6
This policy will be reviewed:	Annually during Term 1
Should serious e-safety incidents take place, the following external persons / agencies will be informed:	Nick Pearce – Technical and Filtering Jo Briscombe – Teaching and Leaning Adviser ICT

The policy is reviewed at least biannually, but also in response to new technologies being introduced or incidents that have taken place. The e-safety working group monitor the impact of the policy using evidence from self-evaluation as identified below.

Scope of the Policy

This policy applies to all members of Raysfield Primary School (including staff, students, volunteers, parents/carers, visitors, governors and community users) who have access to and are users of IT systems. It applies to systems in school and out of school where activities have been set by the school or are using school online systems.

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 relevant to incidents including cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school e.g. remote learning. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate online safety behaviour that take place out of school. The 2011 Education Act increased these powers with regard to the searching for and viewing of electronic devices and deletion of data. In the case of both acts, action can only be taken over issues covered by the School Behaviour Policies.

When dealing with online safety issues, electronic devices will only be searched and deleted with parents. If parents are unavailable the device will be kept securely until a parent can meet to conduct such a search with a senior leader. The school will deal with such incidents within this policy and associated behaviour and anti-bullying polices and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place outside of school.

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

- The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and for monitoring it. This action is delegated to the standards subcommittee.
- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the e-safety leader. The Headteacher is also the designated person for child protection and is trained in e-safety issues and aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

Training and Awareness Raising

There is a planned programme of e-safety training for all staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- An audit of the e-safety training needs of all staff is carried out annually.
- The child protection and e-safety leader receive regular updates through attendance at relevant training such as LA training sessions and by receiving online safety updates from the South Gloucestershire Traded Services.
- All staff, including support staff, receive an annual e-safety update.
- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test processes and update staff on how to deal with issues.
- The e-safety leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.

Induction Processes:

- All new staff receive e-safety training as part of their induction programme.
- Parents are issued with the Acceptable Use Policy (AUP) when joining the school. The staff and governors review this policy annually and the most up to date version is shared on the school's website. IN addition, regular updates regarding e-safety are shared on the whole school's class dojo page.
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy.
- Parents sign whether they are happy for the school to share images & videos of their children

Teaching and Learning

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid e-safety risks.

There is a planned and progressive scheme of work for online safety which is taught in every year group through teaching pupils how to stay safe, how to protect themselves from harm, understand how to manage risk, and how to take responsibility for their own and others safety and how to be responsible users of technology. This is based around the South Gloucestershire Scheme of Work linked to the Digital Literacy Curriculum. Across both Key Stages it covers strands on:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying
- Information literacy
- Self-image and identity
- Digital footprint and reputation
- Creative credit and copyright

The scheme of work is delivered as part of the computing curriculum and additionally through the Jigsaw Scheme of Work. Regular opportunities are taken to reinforce online safety messages in all lessons and to teach pupils to be critically aware and consider the accuracy of the information they access online. Online safety messages are also reinforced through other subjects and through other activities such as assemblies and events. Older pupils are taught to acknowledge the source of information and respect copyright. Pupils are helped to understand the AUP, recognise online safety risks, adopt safe practices, report any issues and keep evidence to support reporting (for older children).

Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Where pupils undertake searching of the internet, staff monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.

If there are educational reasons why a blocked site is needed for learning then staff can request that this be made available to technical staff.

Children new to the school are provided with an overview of expectations when they start.

The following aspects also contribute to our curriculum provision:

• Annual online safety events such as Safer Internet Day are also used to raise awareness.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who are encouraged to reinforce the messages at home.
- Pupils are helped to understand the pupil acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Parents / Carers

Parents have a critical role to play in supporting their children and monitoring their behaviour online, however they may have a limited understanding of the risks and issues and underestimate dangers or be unsure how to deal with them. The school aims to raise awareness and support parents though:

- Curriculum activities.
- Providing clear acceptable use policy guidance.
- Providing newsletter and letters including information on any online safety issues that have been raised in school and how to address these.
- Providing information and web links with current e-safety advice and guidance and where to access support.
- Parents / carers information events.
- Events such as Safer Internet Day
- Communicating reported issues to parents so that they can take appropriate steps to follow these up with their child at home.

The school website contains all relevant polices and also provides information which is relevant for the wider community.

Education – staff and volunteers

All staff receive regular online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training which is regularly updated and reinforced and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- An audit of online safety training needs of staff is carried out regularly, during this training process.
- All new staff receive online safety training and training on relevant policies and expectations as part of their induction programme.
- The online safety lead receive regular updates and external training to support them to do their role.
- Policies relevant to online safety and their updates are discussed in staff meetings.
- The online safety lead provides regular guidance and training to support individuals where required.

Training – governors

Governors take part in online safety training and awareness raising sessions, particularly those governors who are involved with technology and safeguarding. This is offered through:

- Attendance at local authority or regional events
- Attendance at relevant staff training
- Regular newsletter information and access to website information

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- 360 degree safe online self-evaluation tool which is also used to benchmark our provision against other schools.
- Surveys with pupils and staff

Technical Issues

The local authority provides technical and curriculum guidance for e-safety issues. The technical support provider is responsible for ensuring that school infrastructure is secure, and not open to misuse or attack. They ensure that the school meets the requirements of this policy. Users can only access the school's network through an enforced password protection policy, in which passwords are regularly changed. Technical support staff inform Integra Schools IT about any filtering issues.

Password Access to Systems

All our systems are accessed via an individual log in. Users have passwords that include upper and lower case and a number and are encouraged to change these regularly. Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in. The same log in is used to access the computing scheme of work. Access to systems is through groups so that only the relevant group of users can access a resource.

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Integra and this includes a filtering service to limit access to unacceptable material for all users.

Internet access is filtered for all users by South Gloucestershire School IT. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners so as to ensure that "over blocking" does not restrict teaching.

Technical staff monitor internet traffic and report any issues to schools. The school reports issues through logging a call to the service desk at 3838. Any filtering requests for change and issues are also reported immediately to the South Gloucestershire technical team on 3838. Requests from staff for sites to be removed from the filtered list must be approved by the Headteacher and this is logged and documented by a process that is agreed by the Headteacher

The school is currently implementing a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. The iBoss solution being implemented provides the following:

- Active monitoring and automatic alerts for the school to act upon, together with pro-active monitoring by Integra Shools IT to support the school by drawing attention to concerning behaviours, communications or access.
- Enhanced filtering integrated with the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.
- Delegated access to the filtering system allows us to permit or deny access to specific content to support the requirement that "over blocking" does not lead to unnecessary restrictions on what can be taught relating to online teaching and safeguarding - the most severe content will always be filtered.
- Network level filtering which does not rely on any software on the users' devices which could be disabled.
- Ability to produce reports on the websites visited by all young people and adults using our systems.
- The ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up.
- External alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff.
- Automated reporting to ensure that processes are followed without fail.
- Ability to log in from anywhere to see reports via web interface.

Technical Staff - Roles and Responsibilities

Where the local authority provides technical support the "administrator" passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use. The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- There are regular reviews and audits of the safety and security of school IT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school IT systems and are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- School IT technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the downloading of executable files by users.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is detailed regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in our acceptable use agreement.

Use of Digital Images and Video

With the availability of mobile devices and tablets the taking and sharing of images and video are much easier and, if not managed, this could increase the potential risk of misuse. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied.
- Parents sign permission forms to say that they will allow images and videos to be taken of their child and used for educational purposes or to be used for promoting the school.
- Images are only taken and used of individuals where there is a signed permission form in place.
- Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- 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 this is not covered by the Data Protection Act. However in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.

Mobile Technologies

These include mobile phones, tablets or any other device that has similar capabilities. The primary use of these in school is to support learning, teaching and management.

Staff and governors are unable to access wi-fi in school on their personal devices.

Children are not allowed to use their personal devices in school as the school provides access to the technologies to be used for learning. Staff are not allowed to use their personal mobile phones in school while they are teaching. Any use should be restricted to times when children are not present. The only exception to this is in case of emergency during a school trip.

Staff must not use their own mobile phone to take images of children, as the school has devices available for this.

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Personal or sensitive information is not e-mailed but is kept on a secure online site that governors can access via a personal user account.

- Personal email addresses, text messaging, public chat and social networking programmes are not to be used for communications with parents/carers and children.
- An online secure platform is used for pupil learning and this includes secure access to communications tools so that children can learn about these within a limited environment.
- The school uses Facebook, Dojo and Google Classroom to update parents on news and events and this is managed and monitored by the SLT.
- Personal information is also not posted on the school website and only official email addresses are listed for members of staff.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies.
- Personal opinions are not attributed to the school
- Staff personal use of social media where it does not relate to the school, is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.
- The SLT pro-actively monitors the Internet for postings about the school

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones or other camera devices			x				x	
Use of personal 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 open chat rooms / facilities		x						x
Use of school limited chat facilities	x						x	
Use of public instant messaging				x				x
Use of instant messaging across the school community	x						x	
Use of social networking sites				x				x
Use of moderated social networking sites only across the school community				x				x

Use of blogs	x						x	
Use of moderated blogs only across the school community	x						x	

Copyright

The School Business Manager, in conjunction with the school's IT provider, is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs

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.

Transfer of data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office. This also applies to cloud storage used.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix) Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the current Data Protection Legislation
- There is a Senior Information Risk Officer (SIRO) and Information Asset Owner (IAOs) in place.
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- 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.

- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

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.

Reporting and Recording

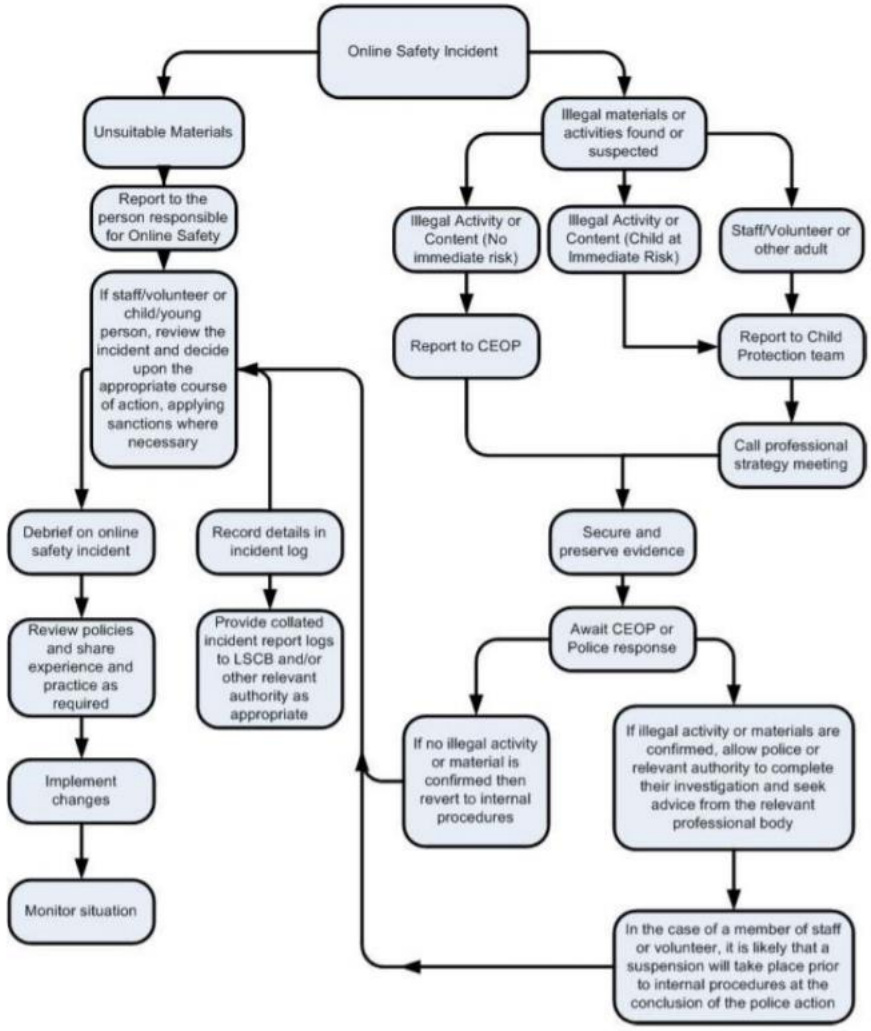
There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

Staff should report online safety issues to the e-safety lead. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and child protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the Headteacher or to the Chair of Governors if the Headteacher is absent or the accusation involves the Headteacher.

Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.

Managing Incidents

In the event of suspicion of an infringement of policy then all the following steps should happen.



- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police. Reporting to the police
- If the content being reviewed includes images of child abuse then monitoring should be stopped and the police informed immediately. Other incidents to be referred to the police are:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

In any of the above, isolate the computer involved as any change to its stage may hamper a police investigation.

If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately. If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team to ensure that this is blocked. Serious incidents are escalated to local authority staff for advice and guidance

Nick Pearce – infrastructure, technical and filtering – 01454 863838
Jo Briscombe – curriculum and policy – 01454 863349
Tina Wilson – LADO allegations against staff and volunteers – 01454 868508
Access and Response Team (ART) – safeguarding / child protection concerns - 01454 866000 (Monday to Friday) and 01454 615165 (Out of hours/Weekends)

For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on helpline@saferinternet.org.uk or 0844 381 4772.

Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

Where appropriate school newsletters and the website are used to provide guidance to staff following an incident in order to prevent further incidents happening. There are defined sanctions in place for any breaches of the acceptable use policies. Suggestions for these can be accessed in SWGfL policy template (Word version with appendices) on pages 17 – 19. Schools are advised to adapt these to suit their own circumstances.

Appendix 1: Roles and Responsibilities

The following roles and responsibilities have been allocated and agreed across the schools.

Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and Acceptable Use policies. E-Safety Governor works with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors
Head teacher and Senior Leaders:	Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. Ensure that there is a system in place for monitoring e-safety Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff Inform the local authority about any serious e-safety issues including filtering Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader:	Lead the e-safety working group and dealing with day to day e-safety issues Lead role in establishing / reviewing e-safety policies / documents, Ensure all staff are aware of the procedures outlined in policies Provide and/or brokering training and advice for staff, Attend updates and liaising with the LA e-safety staff and technical staff, Deal with and log e-safety incidents including changes to filtering, Meet with E-Safety Governor to regularly discuss incidents and review the log Report regularly to Senior Leadership Team
Curriculum Leaders	Ensure e-safety is reflected in teaching programmes where relevant eg anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Participate in any training and awareness raising sessions Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and e-safety policy Report any suspected misuse or problem to the E-Safety Co-ordinator Act professionally and safely when using technology Monitor ICT activity in lessons, extra-curricular and extended school activities Deliver the scheme of work for online safety Use opportunities in the curriculum to reinforce online safety messages
Pupils	Participate in e-safety activities, follow the acceptable use policy and report any suspected misuse Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	Endorse (by signature) the Pupil Acceptable Use Policy. Ensure that their child / children follow acceptable use rules at home. Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet. Access the school website in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events.
Technical Support Provider	Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack. Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data. Inform the head teacher of issues relating to filtering. Keep up to date with e-safety technical information and update others as relevant. Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated. Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

Appendix 2 - Unsuitable / inappropriate activities

The school believes that the activities referred to below are inappropriate for school and that users should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	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 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, 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 SWGfL 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, 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)		x				
On-line gaming (non-educational)					x	
On-line gambling					x	
On-line shopping / commerce					x	
File sharing		x				
Use of social networking sites e.g. Facebook for older users					x	
Use of video broadcasting e.g. Youtube				x		

In conjunction with this policy please read:

- Video Conferencing with Pupils Policy.
- Child Protection Policy (and addendum)
- Safeguarding Policy
- Acceptable Use Policy (staff, parents and pupils)