Courtney Primary School
Nurture, Inspire, Flourish.

E-Safety Policy

Working together to develop lifelong learners with a strong sense of self who are active participants in their communities.

This version dated	Summary of changes	Next review date
February 2024	Update	February 2025

This e-safety policy has been developed, and will be reviewed and monitored by our Computing Subject Leader, Headteacher and the Full Governors Body.

Consultation with the whole school community has taken place previously through staff meetings, pupil conferencing, governors' meetings and the school website / newsletter.

Schedule for Development, Monitoring and Review

Policy ratified by the *Governing Body on::*	
The implementation of this policy will be monitored by:	Computing SL/Headteacher
Monitoring will take place:	Continuously
The *Governing Body* will receive a report on the implementation including reported incidents:	Termly by the Headteacher
This policy will be reviewed:	Annually during Term 6
Esafety incidents will primarily be dealt with by:	Computing Subject Leader/ E-safety Coordinator Lead staff member for Safeguarding Senior Leadership Team
Should serious e-safety incidents take place, the followir external persons / agencies will be informed:	Nick Pearce – Technical and Filtering Jo Briscombe – Teaching and Leaning Adviser ICT

Scope of the Policy

This policy applies to **all** members of the school community (including volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems. It applies in school but also out of school where actions relate directly to school set activity or use of school online systems. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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 such as cyber-bullying, which may take place out of school, but are 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, inform parents / carers of known incidents of inappropriate e-safety behaviour that take place out of school.

This policy should be read alongside the acceptable use policies for staff and pupils.

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 monitoring it. This action is delegated to the Full Governing Body.
- 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 SWGfL and LA training sessions and by receiving regular e-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 our 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.
- A training log kept by the office is used to record when updates and training are delivered- these are further logged on Arbor. Training is currently given as part of a 3 years cycle and in between as and when needed. The Governors are kept informed via the Headteacher's report.

Induction Processes

- All new staff receive e-safety training as part of their induction programme.
- Parents of new children receive an Acceptable Use Agreement about online safety and the school's processes when their child starts school. This agreement should be shared with parents annually and reaffirmed by them.
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the Acceptable Use Agreement.

Curriculum Provision

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 may 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. This is based around the Digital Literacy Curriculum by SWGfL and, across the key stages, 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 following aspects also contribute to our curriculum provision:

- Coverage of the experiences is recorded and staff also check understanding when teaching about online safety.
- Opportunities to reinforce this are mapped to other subjects in the curriculum where appropriate for example, online behaviour is covered in PSHE and communication, copyright and publishing are referenced in English lessons.
- Assemblies are regularly used to reinforce online safety messages.
- 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 we hope will reinforce the messages at home. This agreement will be shared with parents annually and reaffirmed by them.
- In Term 1 pupils are taught about and helped to understand the pupil Acceptable Use Agreement 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 act as good role models in their own use of ICT.
- 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 (see **appendix 2**.)

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to improve e-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, staff and parents.

Parents / Carers

Parents have a critical role to play in supporting their children with managing e-safety risks at home, and reinforcing key messages about e-safety. The school supports parents to do this by:

- Providing clear Acceptable Use Agreement guidance
- Providing regular newsletter and web site articles to keep parents informed
- Providing an awareness raising meeting for parents
- Inviting parents to attend activities such as e-safety week and e-safety assemblies
- Communicating reported issues to parents so that they can take appropriate steps to follow these up with their child at home

Technical Issues
The local authority provides technical and curriculum guidance for e-safety issues for **all** South Gloucestershire schools.

Password Access to Systems

All our systems are accessed via an individual log in. **Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taken using their log in**. 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 Traded Services and this includes a filtering service to limit access to unacceptable material for all users. 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.

Requests from staff for sites to be removed from the filtered list must be approved by the head teacher and this is logged and documented by a process that is agreed by the Headteacher. Any filtering requests about change or issues are reported immediately to the South Gloucestershire technical team on 3838.

Proactive monitoring is in place via a monitoring box provided by SWGfL. Should anyone attempt to access illegal content this is immediately reported to the police. Illegal activity would include attempting to access:

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

For further information on reporting this please **see appendix 4**

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 ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT 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 procedure is in place for the provision of temporary access of “guests” onto the school system. Some guests, for example, members of the PTA, have limited access. Trainee teachers have full access. Community Users/guests who access school computing systems / website / VLE as part of the Extended School provision will be expected to sign a Community User/guests AUA before being provided with access to school systems.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreement.
- 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 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 Agreements:

- 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 Agreement 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 to be taken of their child and used for educational purposes.
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the web site, newsletter or twitter feed. 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 without permission from the parents of any others in the photo being sought. This is clearly detailed in our Acceptable Use Agreement for parents.

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 via the VLE for pupils 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 Agreements.
- Governor communications take place through governor school e-mail accounts. Personal or sensitive information is kept on a secure online site that governors can access to via a personal user account.
- Personal email addresses, personal text messaging, public chat and messaging tools of social networking programmes are not 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 Arbor communications to update parents on news and events and this is managed and monitored by **Kelly Halls** in the school office.
- Personal information is also not posted on the school website and only official email addresses and monitored class email addresses are listed for members of staff. The website is the responsibility of the Headteacher.

- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil Acceptable Use Agreements and the Social Media Policy.

Email / Google Drive

- When using Google Classroom and the Apps, students will use approved class email accounts under supervision of a teacher or parent/guardian.
- Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher and/or guardian.

Distance Learning

- In circumstances where teaching cannot be conducted on the school premises, teachers may use Tapestry in EYFS, Classroom Dojo, Microsoft Teams, Times Tables Rock Stars or other platforms approved by the Head Teacher as platforms (the "Online Platforms") to assist with remote teaching where necessary.
- Videos uploaded via Youtube or Vimeo should be set to Kids Content and made available via web link sent to parents (non-publicly listed).
- The school has signed up to the terms of service of the Online Platforms in use by the school.
- The School has enabled the most up to date security and privacy features which these Online Platforms provide.
- Parents/guardians will be provided with the usernames and passwords and will be expected to monitor their child's use of the Gmail address and Online Platforms.
- Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platforms.

Copyright

The Computing Subject Leader is responsible for making sure that a 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 is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their:

- racial or ethnic origin,
- political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,

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 ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.

- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" as outlined in the policy on the South Gloucestershire IMS Traded Services web site. (see link here to download this policy)
- 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 Data Protection Act (DPA)
- 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 are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- The staff Acceptable Use Agreement clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

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.

- Online safety issues are reported to the E-safety leader via CPOMS.
- In the case of cyberbullying firstly please follow **appendix 5**. Alongside this the school anti-bullying policy will be 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 via CPOMS.
- Staff who are targeted by bullying online report these issues to the head teacher.
- Any member of staff seeing something online that is negative about the school reports this to the head teacher.
- 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.
- Younger pupils are shown how to use *Hector the Protector* (or equivalent as guided by the ICT lead) if they access unsafe content and older pupils are also shown how to report online in case of incidents outside school.
- If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (for South Gloucestershire support 3838).
- If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by ringing 3838 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 865924 -3838
  - Jo Briscombe – Curriculum and Policy 01454 865924 – 3349
  - Leigh Zywek – Safeguarding and Child Protection - 01454 865924 5933

- 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.

There are defined sanctions in place for any breaches of the Acceptable Use Agreements – see **appendix 3**. SWGfL provide clear guidance on what to do if there are suspicions that technology may be being mis-used in order to ensure that the right evidence is collected in a way that does not put the school at risk and these are followed – see **appendix 4.**

Monitoring

The school will monitor the impact of the policy using:

- Logs of reported incidents and responses
- Monitoring logs of internet activity and any network monitoring data
- Regular meetings with digital leaders.
- Surveys / questionnaires of pupils, parents / carers, and staff including non-teaching staff
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the web site is regularly monitored by governors, senior leaders and the office staff to ensure that it complies with this policy and the Acceptable Use Agreement.
- Any other web site, such as the school friends, that is linked to the school name is also regularly monitored to ensure that the school is always presented accurately and professionally.

Appendix 1: Roles and Responsibilities

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 resources are 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	Deal 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 e.g. 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 Leader. Monitor ICT activity in lessons, extra-curricular and extended school activities.
Students / pupils	Participate in e-safety activities, follow the Acceptable Use Agreement 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 Student / Pupil Acceptable Use Agreement. 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 Agreement. 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 the filtering applied by the Grid. 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 Leader 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 AUA before being provided with access to school systems.

Appendix 2: Pupil actions and sanctions framework

Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to COMPUTING Subject Leader and E-Safety Leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓			✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓	✓						✓	✓
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓	✓					✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓	✓			✓	✓	✓	✓
Unauthorised downloading or uploading of files		✓	✓		✓	✓	✓	✓	✓

Allowing others to access school network by sharing username and passwords		✓	✓		✓			✓	
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓			✓	✓	✓	✓
Corrupting or destroying the data of other users	✓	✓						✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓		✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓		✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓		✓			✓	
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓	✓	✓	✓

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓	✓				✓	✓	

Appendix 3 Staff actions and sanctions framework

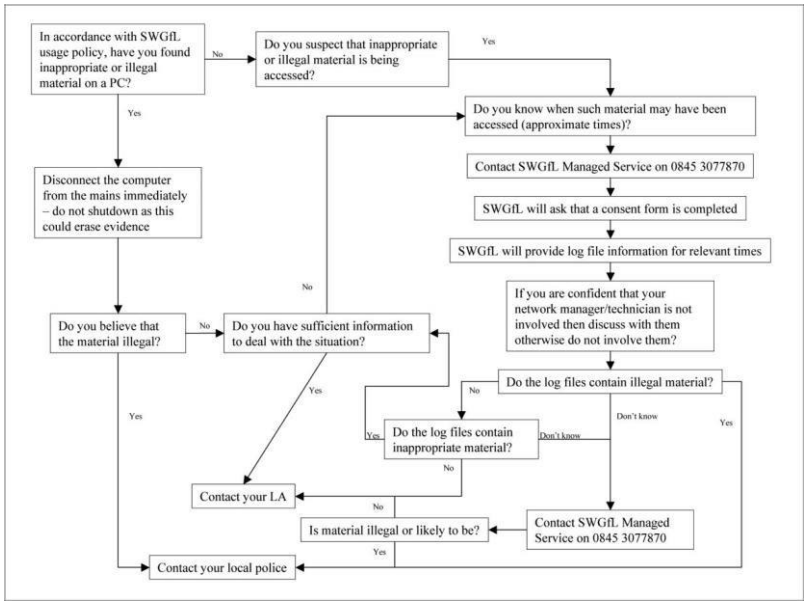
Actions / Sanctions

Incidents:	Refer to line manager	Refer to COMPUTING Subject Leader and E Safety Leader	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).	✓	✓	✓	✓	✓	✓	✓		
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓	✓				✓		
Unauthorised downloading or uploading of files	✓	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓	✓	✓		✓	✓		
Careless use of personal data eg holding or transferring data in an insecure manner	✓	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓		✓	✓		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	✓	✓	✓	✓		✓

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓				✓		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓	✓	✓			✓		
Actions which could compromise the staff member's professional standing	✓	✓	✓	✓			✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓				✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓			✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓					✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓			✓		✓
Breaching copyright or licensing regulations	✓	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓			✓		✓

Appendix 4: SWGfL flow chart for inappropriate or illegal content

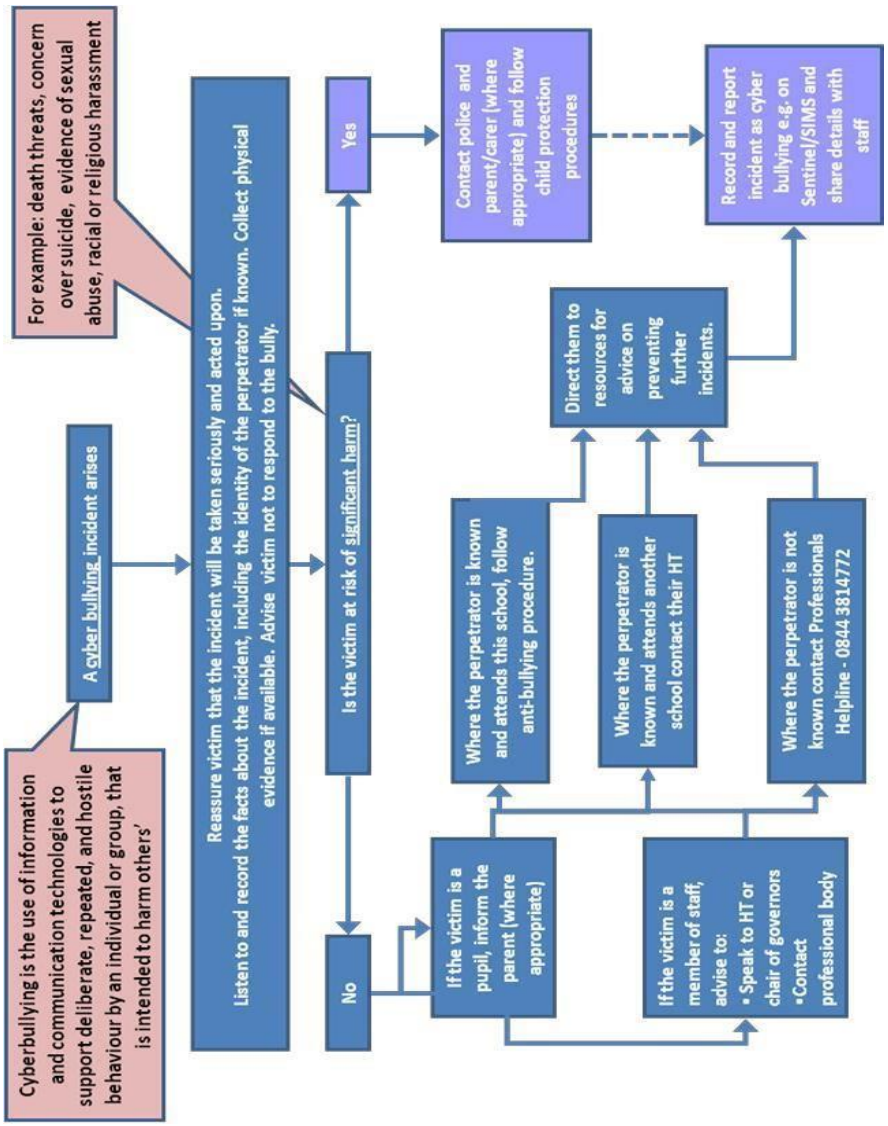
This should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the pol ice and the preservation of evidence.



Appendix 5: Responding to Incidents of Cyberbullying

South Gloucestershir e has produced the following protocol for addressing incidents of cyberbully

Appendix 6: Working practices to comply with GDPR



Staff will be mindful of how they use any document that contains personally identifiable information. This might be a child's full name or a child's first name with additional information that might identify them such as their school, their date of birth or a photograph.

In order to keep this information as secure as possible staff will:

- Only use children's initials or first names in documents / on the walls as much as possible (where there are 2 children with exactly the same name in the class, the first initial of the surname will be used).
- Not make any unnecessary copies of documents (either of electronically or paper) and delete / shred copies when they are no longer required.
- Be careful when printing out documents with personally identifiable information and make sure it is collected from the printer promptly.
- Staff should lock computers when they leave them (either by pressing the windows button and L or by pressing control, alt and delete).
- Personally identifiable information such as supply packs and inhaler lists will be locked away during open school events such as Parents Evenings and PTA events.

Emails

- No personally identifiable information should be emailed to non-south glos. emails.
- Where possible, full names should be replaced with initials or first names in any emails or documents that are sent.

- If sensitive information needs to be emailed to particular staff, the sender should consider putting the information in the body of the email rather than as an attachment as attachments may be downloaded to personal devices.
- If a document contains particularly sensitive information, it should be password protected and the password should be emailed to the relevant staff by a separate email.
- Emails and documents containing sensitive information should be deleted from staff's personal devices once they have been read and are no longer required.
- Staff should check the content of any email chain that they are forwarding as this may contain personally identifiable information. Previous emails should be deleted where not necessary.

Taking paper documents with personally identifiable information off school premises

- Staff will make sure that any paper documents are transported securely.
- Staff will bring any such documents back to school for storing or shredding.

Working on electronic documents at home

- Staff will ensure that any documents with personally identifiable information are only saved on either an encrypted laptop or an encrypted memory stick.
- Staff should use CPOMS in the first instance and attach files to incidents and alert relevant members of safeguarding team.

Any Breaches

- A breach occurs when any information is inputted incorrectly, disclosed to the wrong person, lost or misused.
- It is entirely normal that breaches will occur and the school wishes to foster an open culture where breaches can be reported without any blame.
- A book will be kept in the office and any breaches should be reported to the office.
- The Headteacher and School Business Manager will review these breaches regularly to identify any training needs or necessary changes in practices.