Christ the King Catholic Primary School

Making a difference by

Inspiring a love of life and learning

We build strong foundations within

God's loving hands

OnLine Safety Policy

Author		Annette Johnson / Mary Mainwaring	
Date ratified by Full Governing Body	Dec 25	Chair of Governors	Angela Willian
Start Date	Feb 2020	Headteacher	Mary Mainwaring
Review Date	Dec 27		

Author/Person Responsible	Head Teacher – Mary Mainwaring
Date of Ratification	1st December 2025
Review Group	
Ratification Group	FGB
Monitored By	
Review Frequency	Every 1 years Subject to local education authority and/or national policy change
Review Date	December
Previous Review Amendments/Notes	March 2015
Related Policies	
Chair of Committee Signature	Mary Baskerville

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices:	OnLine Safety Policy	**DATE:**	1st December 25
EIA CARRIED OUT BY	Mary Mainwaring	**EIA APPROVED BY**	Mary Mainwaring

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)	No impact	N/A
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication)	No impact	N/A
Gender reassignment (transsexual)	No impact	N/A
Marriage and civil partnership	No impact	N/A
Pregnancy and maternity	No impact	N/A
Racial groups (consider language, culture, ethnicity including gypsy/traveller groups and asylum seekers)	No impact	N/A
Sex (male, female)	No impact	N/A
Sexual orientation (gay, lesbian, bisexual; actual or perceived)	No impact	N/A

This Online safety policy has been developed, and will be reviewed and monitored, by our school online safety working group which comprises of:

· ICT Subject Leader

· PHSE Subject Leader

· Headteacher

· GDPR Lead

· IT governor representative/Website Governor

And in consultation with the whole school community has taken place through a staff meeting, governors

Monitoring

The school will monitor the impact of the policy through an analysis of:

· Logs of reported incidents and responses

· Monitoring logs of internet activity and any network monitoring data

· Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff

· Monitoring the teaching scheme of work and coverage within the wider 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 the designated governor and senior leaders to ensure that it complies with this policy and the acceptable use policies.

Scope of the Policy

This policy applies to all members of the Christ the King Catholic primary school community (including volunteers, parents/carers, visitors and community users) who have access to or use school ICT systems inside and outside school. The Education and Inspections Act 2006 empowers Head teachers, 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, 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 online safety behaviour that take place out of school. The 2011 Education Act increased these powers with regard to searching for and of the electronic devices found and the deletion of data and related action can only be taken over issues covered by the school behaviour policy. Our behaviour policy states that, when dealing with online safety issues, electronic devices will only be searched and data 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.

This policy should be read alongside the acceptable use policies for staff and pupils, the anti-bullying policy and the behaviour (good relationship) policy.

Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Role	Responsibility
Governors	The DfE guidance "Keeping Children Safe in Education" states: "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety" "Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)" Approve and review the effectiveness of the online safety policy and acceptable use policies Safeguarding governor works with the online safety leader to carry out regular monitoring of online safety incident logs, filtering, changes to filtering and then reports to governors. A member of the governing body will take on the role of Online Safety Governor to include: • regular meetings with the Designated Safeguarding Lead / Online Safety Lead • regularly receiving (collated and anonymised) reports of online safety incidents • checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended) • Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards • reporting to relevant governors group/meeting • Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
Head teacher and Senior Leaders:	Duty of care to ensure the safety (and online safety) of the school community. The Head teacher and at least one other member of SLT should know the procedure to be followed in the event of a serious online safety allegation being made against a member of staff. Ensure that all staff receive suitable CPD to carry out their Online safety roles. Ensure that there is a system in place for monitoring and support of the IT lead who carries out the internal online safety role. Inform the local authority about any serious Online 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.

Online Safety (IT) Leader:	Lead the online safety working group and deal with day to day online safety issues, liaising with the Headteacher/DSL Lead role in establishing / reviewing online safety policies / documents and checking links to other policies, liaising with GDPR lead Ensure all staff are aware of the procedures to follow if there is an online safety incident Working with the Headteacher, to organise relevant training and advice for all school staff and ensure any training is recorded on the safeguarding and health and safety training record. Attend updates and liaise with the LA online safety staff and technical staff Receives reports of online safety incidents and keeps the incident log updated Meet with IT governor to regularly to discuss issues, review the incident log and filtering / changes to filtering log 3 times a year, more if needed. Any serious issues report to Headteacher and Safeguarding Governor immediately Report regularly to SLT Review as needed the online safety teaching programme to deliver the statutory programme of study. Monitor online safety teaching to ensure this is being delivered and is having an impact on pupils' understanding and online behaviour.
Child Protection Safeguarding Lead (DSL)	Keeping Children Safe in Education states that: "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description." They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college" They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online" While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen The DSL will: • hold the lead responsibility for online safety, within their safeguarding role. • Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online • meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out • attend relevant governing body meetings/groups • report regularly to headteacher/senior leadership team • be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded. • liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Curriculum Leaders	Ensure online safety is appropriately reflected in teaching programmes where relevant e.g. Anti-bullying, English: publishing and copyright and is reflected in relevant policies. This will be provided (amend/delete as relevant) through: • a discrete programme • PHSE and SRE programmes • A mapped cross-curricular programme • assemblies and pastoral programmes • through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
Teaching and Support Staff	Ensure they have an up to date awareness of school online safety issues, policies and practices. Have read, understood and signed the Staff Acceptable Use Agreement Policy (AUP) Act in accordance with the AUP and Online safety policy Report any suspected misuse or problem to the Head teacher / online safety leader. In the event that the incident involves the Head teacher report to the governor responsible for safeguarding. Only communicate with pupils / parents / carers professionally through official school systems Ensure online safety issues are embedded in the curriculum and other activities Ensure pupils follow the online safety rules Ensure that the school programme of study for online safety is delivered through their teaching Monitor ICT activity in lessons, extra-curricular and extended school activities Deliver the scheme of work for online safety and ensure children have a good understanding of what they are being taught. Monitor use of digital technologies (mobile devices and cameras etc) in lessons and other school activities where their use if allowed and implement policies about their use. Ensure that students are guided to appropriate sites in pre-planned internet use, that they are aware of how to search more safely and that any unsuitable material that is accessed is dealt with according to school policy. Immediately report any issues in accordance with school policy.

Technical Support Provider (INTEGRA)	The IT Provider is responsible for ensuring that: • they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy • the school technical infrastructure is secure and is not open to misuse or malicious attack • the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body • there is clear, safe, and managed control of user access to networks and devices • they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant • the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action • the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice). • monitoring systems are implemented and regularly updated as agreed in school policies Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack Ensure that the school meets Online safety technical requirements of the LA Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed Ensure that filtering is robust is blocking but does not inhibit learning and teaching Keep up to date with online 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 Head teacher / online 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 take action to prevent spyware and malware.

Students / pupils	Use schools systems in accordance with the Pupil Acceptable Use Policy (SMART Rules) Practice age-appropriate safe searching in order to reduce access to unsafe material Understand how to report online safety issues and do this immediately when an issue arises Know and follow the policies on use of mobile devices and cameras including taking images. Understand the importance of using technologies safely outside school and know that the policy covers actions out of school that are related to their membership of the school Help their friends to keep safe by pointing out any risks and what they could do about them
Parents and carers	Read the school guidance about online safety in the newsletter and on the website and take appropriate action if required to keep their child safe. Endorse (by signature) the Pupil Acceptable Use Policy (R and Y3). Emailed out at the start of each academic year as a reminder Ensure that their child / children follow appropriate acceptable use rules at home Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Keep up to date with issues through school updates and attendance at events Ensure they follow the school policy on taking digital and video images at school events Report any online safety issues that could impact on safeguarding of any children or learning in school so that the school can put in place appropriate measures and use these to inform any changes to teaching
Supply staff	Sign and follow the AUP before being provided with access to school system

Online Safety Policy

The DfE guidance "Keeping Children Safe in Education" states:

"Online safety and the school or college's approach to it should be reflected in the child protection policy"

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements

- is made available to staff at induction and through normal communication channels

· The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it. This action is delegated to the Learning and Leadership committee.

· The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the online safety Leader. The Headteacher is also the designated person for child protection (DSL) and is trained in online 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 online 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 online safety training needs of all staff is carried out.

· The Child Protection and Online Safety Leader receive regular updates through attendance at relevant training such as SWGfL, Andrew Hall Safeguarding and LA training sessions and by receiving regular online safety updates from the South Gloucestershire.

· All staff, including support staff, receive an annual Online 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 Online safety Leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.

· A training log is used to record when updates and training are delivered. This is monitored by the safeguarding governor.

Induction Processes

· All new staff receive online safety training as part of their induction programme.

· Parents of new reception children receive a briefing about online safety and processes when their child starts school.

· There are annual updates to all year groups and parents are asked to re-sign the Acceptable Use Policy

· 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.

Teaching and Learning

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are 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 online safety risks. There is a planned and progressive scheme of work for online safety which is taught at every year group. This is based around the Rising Stars scheme of work and the South Gloucestershire scheme of work and Digital Literacy Curriculum by SWGfL and, across the key stages, covers:

· 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 computing, PSHE and other lessons.

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 a planned programme of 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. Where this is done this a clearly logged with reasons given for this access.

The following aspects also contribute to our curriculum provision:

· Coverage of learning experiences is recorded and staff check understanding when teaching about online safety.

· 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 Policy and this is also communicated to parents who we hope will 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. (SMART Rules)

· 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.

Education – parents / carers and the community

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

· Curriculum activities

· Letters and newsletters including information on any online safety issues that have been raised in school (anonymously recorded) and how to address these

· Parents / carers information evenings

· Events such as Safer Internet Day

· Providing information and web links about where to access support on the website

Parents of children new to the school are provided with an overview of expectations linked to relevant policies including online safety when their child starts school.

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.

· 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. This is completed annually and evaluated

· Surveys with pupils and staff. The results are analysed by members of the SLT

Technical Issues

The local authority provides technical and curriculum guidance for online safety issues for all South Gloucestershire schools as well as providing direct technical support to a large number of schools.

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 taken using their log in.

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 are currently implementing a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education.

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 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 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 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 (to be described) regarding the downloading of executable files by users

· An agreed policy is in place (to be described) 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 Policy.

Use of Digital Images and Video

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyberbullying. 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 publishing their own images 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.

· Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.

· 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

· 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.

· Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.

· 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 General Data Protection Regulation. 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.

· Pupils' work is only published with the permission of pupils and parents / carers.

Mobile Technologies

These might include tablets or any other device that has the capability of accessing the school's wireless network. The primary use of these in school is to support learning, teaching and management.

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; phones must be switched off and kept out of sight. Any use is restricted to times when children are not present and only in the staffroom or school offices. The only exception to this is in case of emergency such as, a lockdown or during a school trip if the school mobile is not accessible or available.

Staff must never use their own mobile phone to take images of children, for example, on a school trip as the school has devices available for this.

Accessing texts and emails via smart watches during lesson time/at work is not permitted, nor is using these devices to take photos.

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. Communications are always professional in tone and content.

· 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.

· Governor communications take place through governor school e-mail accounts. 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 be used for communications with parents/carers and children.

· Tapestry is used for pupil learning within Reception class and this includes communications tools so that teachers and parents can share children's learning within a limited environment.

· MS TEAMS is used to access video meetings

· Personal information is not posted on the school website and only official email addresses are listed for members of staff. The web site is the responsibility of the office administrator.

· Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risk, reporting and issues around social networking forms part of the learning for pupils.

· Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community

· 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 online safety lead pro-actively monitors the Internet for postings about the school.

Copyright

IT lead 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 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 and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 and is:

· 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 and 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 and within the EU. 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.

· 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.

· 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 General Data Protection Regulation (GDPR)

· 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.

· Only cloud storage that meets the requirements laid down by the Information Commissioner's office is used to store personal data.

· 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 ensure that they

· Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse

· Use personal data only on secure password protected computers and devices and log off at the end of every session

· Transfer data using encryption and secure password protected school devices

· The data is encrypted and password protected

· The device is password protected

· The device has approved virus and malware checking software

· The data is securely deleted from the device once finished with.

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 Online 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 (DSL) 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.

The use of Artificial Intelligence (AI) systems in School

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR

- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.

- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools..

- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.

- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.

- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.

- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.

- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.

- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks. (Risk assessment matrices are attached as an appendix)

- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.

- The school will support parents and carers in their understanding of the use of AI in the school

- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI

- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.

- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

the filtering and monitoring provision is reviewed) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

· checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated

- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures

- there is a clear process in place to deal with, and log, requests/approvals for filtering changes

- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

- There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings. (Schools may wish to use e.g. using SWGfL Testfiltering.com to carry out these checks)

- Devices that are provided by the school have school-based filtering applied irrespective of their location.

Monitoring

- The school monitors all network use across all its devices and services.

- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.

- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Cyber Security

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards

- the school will conduct a cyber risk assessment annually and review during the year

- the school, (in partnership with their technology support partner), has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security

- the school has an effective backup and restoration plan in place in the event of cyber attacks with the support of the school IT provider

- the school's governance and IT policies reflect the importance of good cyber security

- staff and Governors receive training on the common cyber security threats and incidents that schools experience

- the school's education programmes include cyber awareness for learners

- the school has a business continuity and incident management plan in place

- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

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

o incidents of 'grooming' behaviour

o the sending of obscene materials to a child

o adult material which potentially breaches the Obscene Publications Act

o criminally racist material

o promotion of terrorism or extremism

o 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 (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 863838

Jo Briscombe – curriculum and policy – 01454 863349

Jon Goddard – 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 https://swgfl.org.uk/resources/online-safety-policy-templates/ (Word version with appendices) on pages 17 – 19. Schools are advised to adapt these to suit their own circumstances.

Appendix A

Online Safety Incident Logging Form

Once this form has been completed, please pass directly to the ICT Coordinator for investigation and resolution.

Date:	**Reporting Member of Staff:**	**Role within School:**

Summary of Incident:		
Computer Name:	**CKT:** **Android:**	**Please circle: Laptop / Desktop (PC) / Tablet**

Resolution / Actions Taken:

Name:		**Signature:**		**Date:**	

Date ICT Governor Contacted:		**By: (member of staff)**	

Appendix B

It is anticipated that incidents of misuse by pupils will be dealt with through the School Behaviour and Disciplinary Policy, Anti-bulling Policies or Child Protection policies as appropriate.

For details of how staff incidents of misuse will be handled please refer to the table below which should be read / used in conjunction with the Staff Disciplinary Policy and procedures.

Incidents:	Refer to Line Manager	Refer to Head Teacher	Refer to Local Authority \ HR	Refer to Police	Refer to Technical	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal See earlier list		✓	✓	✓			✓	✓
Excessive or inappropriate personal use of the internet, social networking sites, instant messaging personal e-mail from school computing equipment		✓				✓		
Unauthorised downloading or uploading of files		✓				✓		
Allowing other to access school network by sharing username and passwords or attempting to access or accessing the school networking using another person's account	✓	✓				✓		
Careless use of personal data eg holding or transferring data via 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 e-mail, social networking, instant messaging or text messaging to carry out digital communications with pupils	✓	✓			✓		✓	✓
Action 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 schools filtering systems		✓	✓		✓		✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓		✓	✓	✓
Breaching copy right or licensing regulations		✓	✓			✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓			✓	✓