St. James' CE Primary School, Haslingden

ONLINE SAFETY POLICY	
Written By	G Lloyd & Online Safety Group
Date	July 2023
Review Date	July 2024

Growing in God's Love, Learning as we go.

We are a safe, loving, supportive, Christian family which values each child's individuality and uniqueness created in the image of God. We nurture the talents given by God to inspire pupils to achieve and succeed, and foster a sense of awe and wonder of God's world

ENDURANCE FORGIVENESS PEACE

FRIENDSHIP TRUST KOINONIA

THANKFULNESS

Online Safety Introduction

Technology and communications are rapidly changing and becoming more sophisticated, with this change comes new ways of being unsafe and feeling threatened. Online Safety (formally e-safety) has become a very important issue that is essential to address in school throughout all areas of the curriculum. This ensures all children remain safe and that the adults remain in control when using the technology. This could be either through the use of computers, accessing the internet, the use of mobile telephones, tablet devices or camera/audio equipment.

Aims of this policy

This policy supplements the Safeguarding Policy in setting out clear guidance and procedures. The policy provides information and clear guidance for all stakeholders and staff within school. At St James' CE Primary School, we aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they feel unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Know what device is appropriate to use and when/where to use it.
- Identify a potential risk or situation from the onset.
- Stay in control and keep personal information private.
- How to take the necessary measures to block and delete accounts, messages and people.

Roles and Responsibilities

All the adults that are involved in the life of the school; whether governors, teaching staff, support staff, technicians, parent-helpers and the community have roles and responsibilities associated with Online Safety. This is in addition to all the pupils that come into contact with computers or electronic devices within the school.

- Governors:
  The Governors are responsible for the approval of the Online Safety Policy and reviewing its effectiveness. Regular meetings and information will be provided to the Governors so they are able to make the correct recommendation. They will also be able to carry out regular monitoring of Online Safety incident logs when required.

- Head Teacher and Senior Leadership Team (SLT):
  The Head Teacher is responsible for ensuring the safety, including Online Safety, of the members of the school community. The day to day managing of the Online Safety Curriculum will be delegated to the Online Safety Co-ordinator and Computing Curriculum Leader. The Head Teacher and Senior Leadership Team are responsible for ensuring that all staff and Online Safety Co-ordinator receive the correct and suitable Continuing Professional Development (CPD).

  The Head Teacher and Senior Leadership Team will ensure that there is a system in place to monitor the usage of internet and other technologies and that the person who carries out the internal Online Safety monitoring receives support and is also monitored. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

  The Head Teacher and Senior Leadership Team will ensure that they receive regular updates and reports from the Online Safety Co-ordinator.

  The Head Teacher and members of the Senior Leadership Team are to ensure they know the correct procedures that must be followed when a serious allegation has been made by a child or one regarding a member of staff.

- Online Safety Co-ordinator:
  The Online Safety Co-ordinator will:

- take day to day responsibility for the Online Safety Curriculum and has a leading role in establishing and reviewing the school Online Safety policies/documents.
- Support the Senior Leadership Team in ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place and will provide training and advice for all staff.
- liaise with the Local Authority, relevant external agencies and ICT technical support staff.
- review reports of Online Safety incidents and evaluates the log of incidents to inform future Online Safety developments.
- liaise regularly with Governors to discuss current issues, review incident logs and filtering/change control logs and reports regularly to Senior Leadership Team.
- conduct annual online safety assemblies/lessons/activities for all children.
- send home online safety advice via newsletters or emails throughout the academic year that have a focus for both parents and children.

- Technical Staff:
  The ICT technical support staff are responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- the school meets the Online Safety technical requirements outlined in the Lancashire Online Safety Policy Guidance.
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- he/she keeps up to date with relevant Online Safety technical information and guidance in order to carry out their role effectively.
- monitoring software/ systems are implemented and updated regularly.
  - Teaching and Support Staff:

Teaching and Support Staff are responsible for:

- ensuring they stay up to date with current Online Safety matters and policies and practice. o reading, understanding and complying with the school's Acceptable Use Policy (AUP).
- reporting any misuse by children or staff to the Online Safety Co-ordinator/Head Teacher for further investigation via the CPOMs software.
- emailing any technical problems to the school's Bursar who will in turn log these with the ICT technical support staff.
- ensuring that any digital communications with pupils, for example email and learning platforms, should be strictly professional and only carried out using school systems.
- following the current computing scheme adopted by the school* to ensure that the teaching of Online Safety is embedded throughout the computing curriculum.
- that pupils understand and follow the AUP and Online Safety policy.
- being aware of Online Safety issues relating to the use of mobile phones, cameras, smart watches, websites, games and handheld devices/wearable technology and that they monitor their use and implement current school policies with regard to these devices.

**Currently, the school has adopted the Purple Mash Computing scheme for Years EYFS to 6.*

- Designated Senior Leader (DSL)

The DSL needs to ensure that they are fully trained in Online Safety issues and are aware that serious child protection issues could occur due to:

o Cyber-bullying

o Sharing of personal data/photographs

o Inappropriate online conduct with adults/strangers

o Potential or actual incidents of grooming

- Pupils/Students:

Pupils and students are responsible for:

- Knowing and acting accordingly to the school's AUP.
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and know how to report them.
- Knowing the policy on mobile phones, digital cameras, smart watches and other hand held devices/wearable technology and to realise these can be used for cyber-bullying.
- Understanding that the Online Safety policy also covers their actions out of school, especially if related to a member of the school community.

- Parents/Carers:

Parents and carers have the responsibility to ensure that their children use their internet enabled devices appropriately and do not misuse these technologies. Parents are made aware of the school's AUP and Online Safety Policy through the induction pack, school website and the Parent, Carer and Child Handbook.

The educating and/or providing further information around the AUP and Online Safety Policy is provided through newsletters, assemblies and links online via the school's website.

Education

All children will receive planned Online Safety lessons throughout Computing and PSHE lessons. These lessons will be regularly revisited and revised to suit the new technologies in and out of school. Key messages will be delivered through a variety of lessons, worships and weekly newsletters to ensure all children are aware of the matter. They will also be taught to question the validity of the information they find online.

Parents receive information via parent's evenings, weekly Online Safety posts, newsletters and links via the school's website.

It is each staff member's wider professional responsibility under the safeguarding of children to read and understand the Online Safety Policy. All staff are required to read and understand the elements of Online Safety stated within the latest version of Keeping Children Safe in Education (KCSIE) as part of their wider Safeguarding responsibility. All new staff are directed to read the Online Safety Policy Document as part of the induction process to ensure they are fully aware and understand the Online Safety. Once in receipt of the policy document, either in a physical form or directed to its online form, it is presumed they understand the policy, unless they seek further advice.

The Online Safety Co-ordinator will be able to respond to regular updates provided by Lancashire LEA or other training schemes and report back to staff any new issues that they need to be aware of by either email or an arranged meeting. The Online Safety Co-ordinator will provide guidance for any member of staff that seeks it.

Governors will attend regular meetings which will provide information about Online Safety.

Technical

St James' CE Primary School receives a filtered broadband service. This service is intended to stop users from accessing any material that would be regarded as inappropriate for the learning environment or illegal.

The service is managed by ***** and the school's SLT with oversight from the Governor responsible for IT. This allows for the service to be flexible, so the school can have ownership of what else needs to be filtered as technology advances. It also has the advantage of being able to introduce different policies for different user groups and devices in the school.

The broadband is supplied by ***** and further information can be found at www.****.

***** is our school's filtering solution. It is a hardware-based content filtering solution built to provide schools with an even more comprehensive content filtering solution than our Cloud option offers.

Along with all the basic features of *****, ***** offers an even greater level of control over the school's filtering. The school is able to filter the content of both HTTPS and HTTP sites in the same way, while establishing different filtering profiles for any group of users, computers, or user accounts. It also gives the school a tool for monitoring the content that is being requested on the internet.

The monitoring of pupil and staff devices is done via the ***** Software. The software is set up with both default and bespoke alerts which notify a member of the Senior Leadership Team if a breach occurs.

All personal data will be stored accordingly to the Personal Data Act 1998. Staff must use personal data on secure password protected machines and other devices, ensuring that they 'log off' at the end of any session. This will then minimise any chance of the data being seen by others.

It is prohibited for staff to store photographs of children or paperwork that is confidential on any system other than the laptops, iPads provided by the school or their professional OneDrive account. Photographs can be stored on the OneDrive cloud-based storage system as a method of printing but should be deleted once they are printed. Certain photographs can be stored on OneDrive throughout the year with the Head's permission. An example of this are photographs used for the Behaviour Traffic Lights in school. These should be deleted, however, once the child leaves the school or moves to a different class.

The use of smart watches is permitted in school for both adults and children providing they cannot take photographs or record video.

It is the responsibility of all teaching/support/welfare staff to ensure their laptop or tablet device is locked whenever their device is left unattended.

When a child or class are using a teacher's iPad, it is the responsibility of the teacher or support member of staff to ensure that the iPad is locked to that one application by activating the Guided Access function within the settings. There may be occasions where the child/class have this deactivated – for example: when children are doing a task that requires the multitasking on two or more applications. When deactivated, the teacher should be able to easily view the screen of the iPad.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum. In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the pupils visit and should remind the children what to do in the event of seeing an inappropriate image prior to starting the lesson.

It is accepted that from time to time, for good educational reasons, students may need to research topics during lessons (e.g. weapons - which could be part of a study on the Roman Army) that would normally result in internet searches being blocked. In such a situation, staff should obtain permission from a member of the school's SLT and then request a temporary removal of those sites from the filtered list for the period of study by contacting the school's Business Manager. Any request to do so, should have clear reasons to support the need of these websites.

Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information. Additionally, children should be taught the school's adopted approach for when they come into contact with inappropriate material. To promote online safety within the school, the children are taught a message. There is a different message for KS1 and KS2 to compliment their level of technological understanding. Children should be reminded of the appropriate message throughout the year and within all online safety or computing lessons. It is within Year 3 that the teaching of the new KS2 phrase should take place.

KS1 Online Safety Message: If it upsets you, switch off the screen and tell an adult.

KS2 Online Safety Message: Save it, Block it, Report It.

Reporting

All staff must report any safeguarding concerns regarding online safety through the school's reporting system, CPOMS and a DSL notified as soon as possible.

Further detail on the school's Safeguarding Report Procedure can be found within the school's Safegurading Policy.

Communications

This is an area which is rapidly developing and will need to be constantly revisited as technology advances and changes. St James' CE Primary School recognises that different communications can have the potential to enhance learning and therefore can be a powerful tool. We are also aware of the risks that may come with these in regards to Online Safety.

Table 1.1 outlines how these communication devices are to be used by both staff and children at school. Some applications are permitted at certain times, but are strictly for education purposes. If there are any queries/uncertainty, then guidance should be sought by either the Head Teacher, SLT School's Use of Social Media

As a school, we believe that it is important to have a presence on social media. We believe that as a school, we can exemplify a positive presence online by acting in a responsibly way for others to emulate.

The school's website, Class Dojo and Facebook account allows quick communication with a large number of parents, carers and members of the school's wider community when compared with more traditional methods. It also allows for the sharing of digital media where appropriate.

Teachers have access to their own Class Dojo pages linked to the learning of their class or a subject area. Staff should consider and observe their professional teaching standards and professional code of conduct when posting or commenting on any social media.

The posting on the school's official Facebook account is the responsibility of the School's Deputy Headteacher. At all times, policy advice and GDPR must be followed. This means that several policies need referring to.

Table 1.1 – Communication methods available and what is allowed/not allowed by staff/pupils.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X(*1)						X
Taking photos on mobile phones when children are on the premises.				X (*2)				X
Taking photos on provided cameras.		X				X		
Use of hand held devices eg PDAs, iPads, etc.		X				X		
Use of personal email addresses in school, or on school network				X (*3)				X
Use of cloud based storage systems other than OneDrive				X (*4)				X
Use of school email for personal emails		X						X
Use of chat rooms / facilities				X				X
Use of instant messaging		X						X
Use of social networking sites		X						X
Use of blogs		X					X	

**1 – In restricted areas, e.g. staffroom and offices.*

**2 – Pictures of children should never be taken on personal phones.*

**3 – All staff have a @haslingden-st-james.lancs.sch.uk email upon induction.*

**4 – All staff should use the OneDrive cloud storage account linked to their @haslingden-st-james.lancs.sch.uk email account.*

Use of Digital Video and Digital Images:

The developments of digital images and videos have significant benefits within the curriculum and can enhance learning. Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet and on social networking sites.

Members of staff are allowed to take digital/video images to support educational purposes, but must follow school policies concerning the sharing, distribution and publication of those images, as well as personal information. Further details can be found in the school's policies and procedures related to the General Data Protection Regulation (GDPR). The school has a clearly displayed list which states where parental permission has been declined for specific pupils to not have their photos taken and/or published online. Any photographic image should only be taken on school equipment. The use of personal photographic equipment by staff should <u>not</u> be used for such purposes.

Care should be taken that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils, teachers, or the school into disrepute.

Pupils' full names will not be used anywhere on the website or in blogs and particularly not associated with photographs on there.

Permission must be obtained from the parent or carer of any child before pictures are published on the website. Written permission is provided for every child that starts school to indicate whether the parent or carer allows their child to be photographed.

St James' CE Primary School will always comply with the Data Protection Act 1998 and 2018 in regard to personal information, digital images and videos.

It is strongly advised that members of staff should delete any photographs that are no longer required. Under no circumstances should photographs be transferred to a USB storage device, portable hard drive that is due to leave the school premises or uploaded onto a third-party commercial cloud-based storage system other than OneDrive.

Table 1.2 outlines what activities are acceptable and unacceptable for both staff and pupils. All users of the computers will be made aware of what is acceptable or not by the AUP. If unacceptable use is conducted, the correct procedures and sanctions are in place.

It is expected that all users will be responsible and safe users of ICT, who understand the policy and work within it. However, at times an infringement of the policy may occur whether through carelessness or, very rarely, deliberately.

Examples of illegal activity:

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

If any apparent or actual misuse appears to involve illegal activity, like those examples listed above, the correct reporting procedure is in place and all staff are aware to inform the Head Teacher, Child Protection Officer and/or the SLT immediately, who will then investigate the matter.

All children will be made aware of the importance to report any incident to either an adult at school that they can trust.

If an incident has occurred due to carelessness, which will be more likely the case, this will to be investigated and the correct sanctions will be implemented. All users within the school are aware that there is a monitoring system that is in place and is sensitive enough to pick up slight infringements of the policy.

Table 1.3 indicates how different offences will be dealt with regarding both pupils and staff. In all cases, the Head Teacher when notified will decide what action to take and whether the incident needs further action, e.g. reporting to police, Local Authority.

Table 1.2: Acceptable to illegal use of ICT on school premises:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images				X	X
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation				X	X
	adult material that potentially breaches the Obscene Publications Act in the UK				X	X
	criminally racist material in UK				X	X
	pornography				X	
	promotion of any kind of discrimination				X	X
	promotion of racial or religious hatred				X	X
	threatening behaviour, including promotion of physical violence or mental harm				X	X
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	X
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Lancashire LEA and/or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					X	
On-line gaming (educational)		X				
On-line gaming (non educational)			x	x		

On-line gambling (on school premises)		x	x		
On-line shopping / commerce (in school time)		X	X		
File sharing (Peer-to-peer file sharing, not including the use of Cloud services)				X	
Use of social networking sites		X			

Table 1.3: Dealing with various breaches of the policy by Students/Pupils. Incidents	Refer to class teacher	Refer to Head Teacher and/or SLT	Refer to Police	Refer to technical support staff for action– EG:	Inform parents/ carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X			X	X	X	
Unauthorised use of mobile phone / digital camera / other handheld device	X	X			X	X	X	
Unauthorised use of social networking / instant messaging / personal email	X	X		X	X	X	X	
Unauthorised downloading or uploading of files	X	X		X	X	X	X	
Allowing others to access school network by sharing username and passwords	X	X		X	X	X	X	
Attempting to access or accessing the school network, using another student's / pupil's account		X		X	X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff		X		X	X	X	X	
Corrupting or destroying the data of other users		X		X		X	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X	X	
Continued infringements of the above, following previous warnings or sanctions		X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X		X

Using proxy sites or other means to subvert the school's filtering system		X		X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X			X	
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X	X	X	X	

Table 1.4: Dealing with various breaches of the policy by Staff.

Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X		X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X	X		X	X	X	X
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X				X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X			X		X
Deliberate actions to breach data protection or network security rules		X	X					X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X			X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X	X				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X			X	X	X

Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X					X
Using proxy sites or other means to subvert the school's filtering system		X	X			X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X		X		X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X				X	X

Monitoring and Review and Policy Ownership

Working with Parents

Our school seeks to work in partnership with parents to provide effective Online Safety. Parents need to know that the school's Online Safety programme will complement and support their role as parents and that they can be actively involved in the determination of the school's policy.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.