All Saints RC Primary

e-Safety Policy

November 2023

Contents

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who

have access to and are users of school ICT systems, both in and out of the school.

Development / Monitoring / Review of this Policy

This e-Safety policy will be shared with Governors, Staff, Parents and children as well as other community users of IT in the school.
Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Governing Body / Governors Sub Committee on:*	……Nov……2023
The implementation of this e-Safety policy will be monitored by the:	*ICT subject leader: Adam Davies*
Monitoring will take place at regular intervals:	Termly 2023.24
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	*Autumn Term*
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	*Nov 2024*
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	*J.Price Headteacher* *R Meadows Deputy Headteacher* *F Bsaini (DSP)* *S.Dixon Blaenau Gwent safeguarding Officer.*

The school will monitor the impact of the policy using:

- *Internal monitoring data for network activity*
- *Surveys / questionnaires of* ➢ *students / pupils*
  - ➢ parents / carers
  - ➢ *staff*

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals[1] and groups within the school :

Governors:

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governing body / Governor's sub-committee* receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of eSafety Governor[2] to include:

- *regular meetings with the e-Safety Co-ordinator / Officer*
- *regular monitoring of e-Safety incident logs*
- *regular monitoring of filtering / change control logs (where possible)*

[1] In a small school some of the roles described below may be combined, though it is important to ensure that there is sufficient "separation of responsibility" should this be the case.

[2] It is suggested that the role may be combined with that of the Safeguarding Governor

- *reporting to relevant Governors / sub-committee / meeting*

Headteacher / Principal and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including e-Safety) of members of the school community**; the day to day responsibility for e-Safety will be delegated to the ICT subject leader/Deputy Headteacher.
- **The Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.**[3]
- **Headteacher and Deputy Headteacher** *and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.*
- **Headteacher and Deputy Headteacher** *will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the e-Safety Co-ordinator.*

e-Safety Coordinator / Officer: Mr. Adam Davies

The *e-Safety Coordinator / Officer*

- leads the e-Safety committee
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with (school) technical staff
- receives reports of e-Safety incidents[4] and creates a log of incidents to inform future e-Safety developments.
- meets regularly with e-Safety *Governor* to discuss current issues, review incident logs and if possible, filtering / change control logs
- attends relevant meeting / sub-committee of *Governors*
- reports regularly to the Headteacher and Senior Leadership Team

Network Manager / Technical staff:

NOTE: If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety policy and procedures.

The *Network Manager / Technical Staff* (or managed service provider) is responsible for ensuring:

[3] see flow chart on dealing with e-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures.

[4] The school will need to decide how these incidents will be dealt with and whether the investigation / action will be the responsibility of the e-Safety Co-ordinator / Officer or another member of staff eg Headteacher / Principal / Senior Leader / Safeguarding Officer / Class teacher / Head of Year etc.

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets (as a minimum) the required e-Safety technical requirements as identified by the *Local Authority or other relevant body* and also the e-Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- *that the filtering policy (if one exists), 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)
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher / Principal / Senior Leader; e-Safety Coordinator*
- *that (if present) monitoring software / systems are implemented and updated as agreed in school policies*

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP / AUA)**
- **they report any suspected misuse or problem to the *Headteacher / Principal / Senior Leader ; e-Safety Coordinator / Officer* for investigation / action**
- **all digital communications with students / pupils / parents / carers should be on a professional level** *and only carried out using official school systems*
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-Safety and acceptable use *agreements / policies*
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / 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*
- As per statutory guidelines, the e-Safety element of the Digital literacy and Citizenship strand of the Digital Competence Framework is to be taught as part of the new curriculum.

Safeguarding Designated Person

NOTE: It is important to emphasise that these are safeguarding **issues**, not technical issues; the technology provides additional means for safeguarding issues to develop. Some schools may choose to combine the role of Safeguarding Officer and e-Safety Officer.

The *Safeguarding Designated Person* should be trained in e-Safety issues and be aware of the potential for serious safeguarding issues to arise from:

-
- sharing of personal data[5]
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
  cyber-bullying

e-Safety Group

The e-Safety Group[6] provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-Safety and monitoring the e-Safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the e-Safety Group (*or other relevant group*) will assist the *e-Safety Coordinator / Officer (or other relevant person, as above)* with:

- the production / review / monitoring of the school e-Safety policy / documents.
- *the production / review / monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes.*
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs where possible
- consulting stakeholders – including parents / carers and the students / pupils about the e-Safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

An e-Safety Group Terms of Reference Template can be found in the appendices (B4)

Students / pupils:

- **are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

[5] Appendix B2

[6] Schools will need to decide the membership of the e-Safety group. It is recommended that the group should include representation from students / pupils and parents / carers.

-

Parents / Carers

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

- digital and video images taken at school events
  access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. A Community Users Acceptable Use Agreement Template can be found in the appendices (A6)

Policy Statements

Education – young people

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in e-Safety is therefore an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience.

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

- **A planned e-Safety curriculum should be provided as part of ICT / Computing / PSE / Digital Literacy lessons or other lessons and should be regularly revisited**
- **Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students / 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

-

Education – parents / carers

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

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

- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
  Reference to the relevant web sites / publications eg https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Education – The Wider Community

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

- *Providing family learning courses in use of new digital technologies, digital literacy and e-Safety*
- *e-Safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school VLE / website will provide e-Safety information for the wider community*
- *Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-Safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk)*

Education & Training – Staff / Volunteers

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows part of in service training and with access to external providers.

- **A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify e-Safety as a training need within the performance management process.*
- **All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Agreements.**
- *The e-Safety Coordinator will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This e-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.*
- *The e-Safety Coordinator will provide advice / guidance / training to individuals as required.*

Training – Governors

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any sub-committee e-Safety / health and safety / safeguarding . This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).

-
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school e-Safety Policy / Acceptable Use Agreements. The school should also check their Local Authority / other relevant body policies on these technical issues if the service is not provided by the Authority.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their eSafety responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users will be provided with a username and secure password** by *Mrs N. Davies* *who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password** *and will be required to change their password at frequent intervals.*
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the *Headteacher / Principal* or other nominated senior leader and kept in a secure place (eg school safe)**
- Mr J. Price **is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Websense will provide filtering for pupil access. There is a clear process in place to deal with requests for filtering changes (see appendix for more details).
- *The school has provided enhanced / differentiated user-level filtering.*
- *Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place* for reports to Mrs N Davies and Mr J. Price *of any actual / potential technical incident / security breach. This is then reported to the Headteacher.*
- Appropriate security measures are in place through the local authority (SLA) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off*

- *the school site unless safely encrypted or otherwise secured.* (see School Personal Data Policy Template in the appendix for further detail)

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-Safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD must not introduce vulnerabilities into existing secure environments.

A device may be a privately owned smartphone, tablet, notebook / laptop or other new technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet including the school's (Hwb+) learning platform and other cloud based services such as email and data storage. The device may typically also be used for the taking of images, for the recording of sounds or video and for generating and storing a wide range of other types of data (often as a result of using an app).

The absolute key to approaching BYOD is that the students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of

whether the device they use is user or school owned. This understanding then underpins further conventions around acceptable use of both the devices and of the wider network.

Potential Benefits of BYOD

Research is highlighting the widespread uptake of portable, wireless enabled electronic devices amongst adults and children of all ages. This technology exists as part of their everyday digital world and by allowing them to use these devices freely in school, the school is bringing that familiar digital life into the school classroom. Learners will no longer have to 'power down' when they walk through the doors of the school and can engage with and own their learning more effectively. BYOD has the potential to maximise the huge investments that have been made in schools' infrastructure and allows for greater opportunity to engage with learning technologies.

Considerations

Schools do need to be aware that access to such devices is not yet ubiquitous and that any BYOD implementation will need to address issues over equality of access for all learners.

BYOD brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement BYOD successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

The school must develop a new, strengthened Acceptable Use Agreement for staff, students and parents/carers (template policy statements are found below) as a minimum, and will need to support teaching staff, learners and parents through this shift in approach.

The essential principle of safe and responsible use of the internet and learning technologies sits with the understanding that this technology is allowed primarily for educational purposes. Online safety should already be enshrined in existing e-Safety awareness programmes and in the school's current Acceptable Use documentation. The BYOD policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use (of the internet) Policy, policies around theft or malicious damage and the Behaviour Policy.

(see appendix B3 for a more detailed BYOD Policy Template)

Use of digital and video images

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

- **When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal

use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students / pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (*
- *Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.*

Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights • Secure
- Only transferred to others with adequate protection.
- **The school will comply with the new GDPR TBC BG LA 2022.**

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (**see Privacy Notice section in the appendix)
- **It has a Data Protection Policy** (2023)
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs) Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

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

- the data must be encrypted and password protected
- the device must be password protected the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

See The Personal Data Handling Policy Template in appendix B2 provides more detailed guidance on the school's responsibilities and on good practice.

Communications

This is an area of rapidly developing technologies and uses.
A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults			Students / Pupils				
	Allowed	Allowed at certain times	Not allowed for staff	Allowed	Allowed at certain times	owed with staff permission	Not allowed
Mobile phones may be brought to school	/							/
Use of mobile phones in lessons			/					/
Use of mobile phones in social time		/						/
Taking photos on mobile phones / cameras			/					/
Use of other mobile devices eg tablets, gaming devices			/					/
Use of personal email addresses in school, or on school network		/						/
Use of school email for personal emails			/					/
Use of messaging apps		/						/
Use of social media			/					/
Use of blogs			/					/

When using communication technologies the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only* take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at Foundation Phase, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use. (Schools may choose to use group or class email addresses for younger age groups eg. At FP)
- Students / pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

(See Appendix A, B C)

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions

		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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing				X	
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting eg Youtube				X	

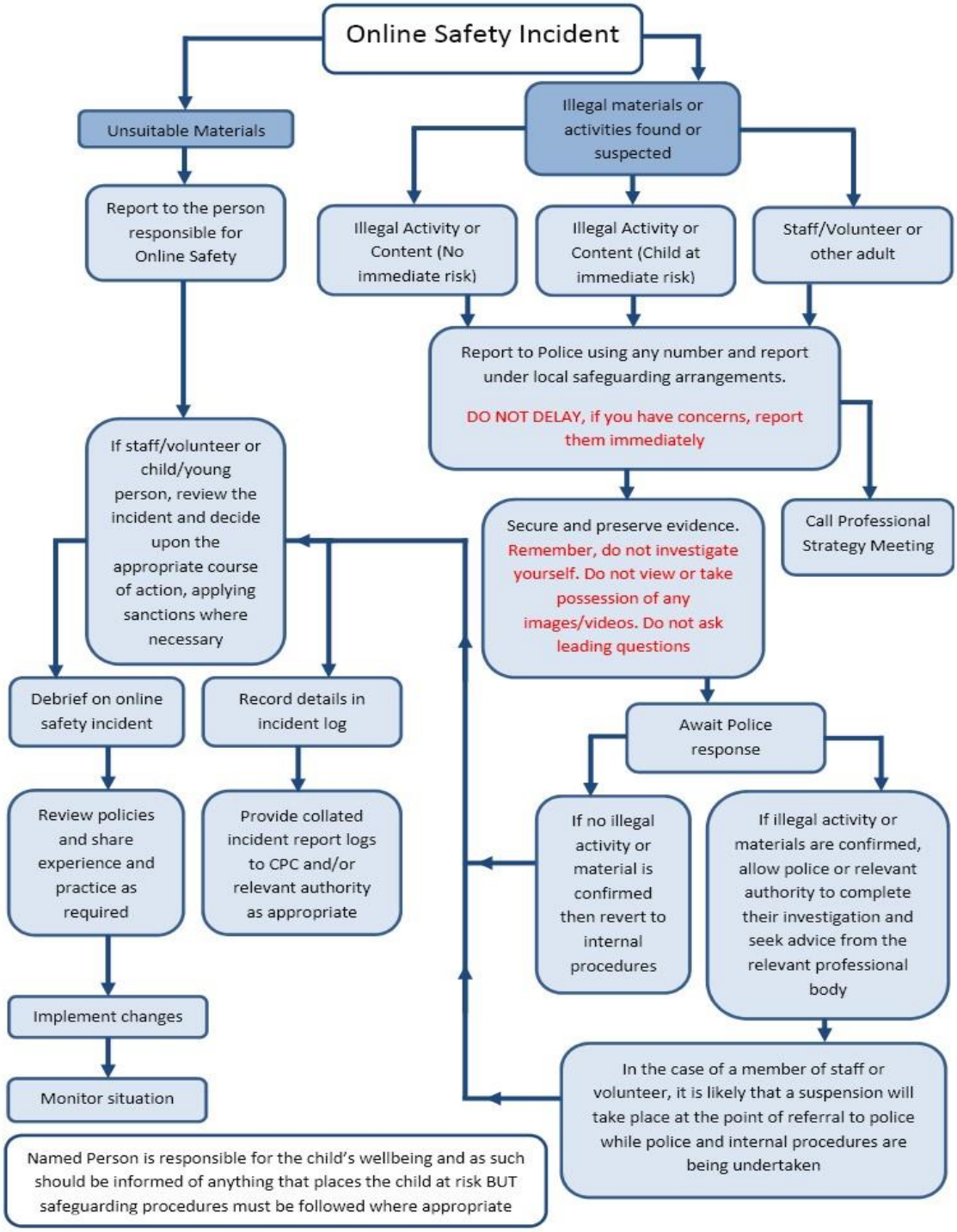
(The school should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools to decide their own responses)

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. **In the event of suspicion, all steps in this procedure should be followed:**

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

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

School Actions

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

Students / Pupils Actions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction 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					
Unauthorised use of non-educational sites during lessons			X						
Unauthorised use of mobile phone / digital camera / other mobile device			X						
Unauthorised use of social media / messaging apps / personal email			X						
Unauthorised downloading or uploading of files			X						
Allowing others to access school network by sharing username and passwords			X						
Attempting to access or accessing the school network, using another student's / pupil's account			X						
Attempting to access or accessing the school network, using the account of a member of staff			X						
Corrupting or destroying the data of other users			X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X						
Continued infringements of the above, following previous warnings or sanctions			X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						
Using proxy sites or other means to subvert the school's 's filtering system			X						

Accidentally accessing offensive or pornographic material and failing to report the incident			X	X					
Deliberately accessing or trying to access offensive or pornographic material			X	X					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X						

Staff Actions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	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				
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files		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					
Careless use of personal data eg holding or transferring data in an insecure manner		X	X					
Deliberate actions to breach data protection or network security rules		X	X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		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					
Using proxy sites or other means to subvert the school's 's filtering system		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
Breaching copyright or licensing regulations		X	X					
Continued infringements of the above, following previous warnings or sanctions		X	X					X

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from: https://hwb.wales.gov.uk

Acknowledgements

WG and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School e-Safety Policy Template and of the 360 degree safe e-Safety Self Review Tool:

- Members of the SWGfL e-Safety Group
- Representatives of SW Local Authorities
- Representatives from a range of Welsh schools involved in consultation and pilot groups
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Approved by Governors: Nov 2023

Signed: Mrs P Zagozda, Mr J Price

Review Date: Nov 2024

Appendix (A)

A1 PERSONAL USE OF SOCIAL MEDIA

A1.1 Staff members must not identify themselves as employees of All Saints Catholic Primary School or service providers for the school in their personal webspace. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

A1.2 Staff members must not have contact through any personal social medium with any pupil, whether from All Saints Catholic Primary School or any other school, unless the pupils are family members. Staff may not be friends with any ex-student until they reach the age of 20.

A1.3 All Saints Catholic Primary School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way

A1.4 Staff members must not have any contact with pupils" family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

A1.5 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites created according to the requirements specified in section 7 and Appendix (2).

A1.6 Staff members must decline „friend requests" from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become „friends" of the official school site.

A1.7 On leaving All Saints Catholic Primary School service, staff members must not contact All Saints RC Primary School pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

A1.8 Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues and other parties and school corporate information must not be discussed on their personal webspace.

A1.9 Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school uniforms or clothing with school logos or images identifying sensitive school premises must not be published on personal webspace.

A1.10 School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

A1.11 Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer"s IP address and the intervention will, therefore, appear as if it comes from the employer itself.

A1.12 All Saints Catholic Primary School only permits limited personal use of social media while at work. Access to social media sites for personal reasons is not allowed between 9am and 5pm. There is a daily quota of 30 minutes to access these sites outside these hours. However, staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the school's time. Caution is advised when inviting work colleagues to be "friends" in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.
Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

A2 USING SOCIAL MEDIA ON BEHALF OF All SAINTS CATHOLIC PRIMARY SCHOOL

A2.1 Staff members can only use official school sites for communicating with pupils or to enable pupils to communicate with one another.

A2.2 There must be a strong pedagogical or business reason for creating official school sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.

A2.3 Official school sites must be created only according to the requirements specified in Appendix 1 of this Policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

A2.4 Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

A3 MONITORING OF INTERNET USE

A 3.1 All Saints Catholic Primary School monitors usage of its internet and email services without prior notification or authorisation from users.

A 3.2 Users of All Saints Catholic Primary email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school"s ICT system.

A4 BREACHES OF THE POLICY

A4.1 Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with All Saints Catholic Primary School Disciplinary Policy and Procedure.

A4.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of All Saints Catholic Primary School or any illegal acts or acts that render All saints RC Primary
School liable to third parties may result in disciplinary action or dismissal.
Contracted providers of All Saints Catholic Primary School services must inform the school ICT

Coordinator and/or the headteacher, immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school. Any action against breaches should be according to contractors" internal disciplinary procedures.

Appendix (B)

Requirements for creating social media sites on behalf of All Saints Catholic Primary School B1 CREATION OF SITES

.

B2.1 Staff members or any associated body working on behalf of All Saints Catholic Primary School, participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of All Saints Catholic Primary School.

B.2.2 Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

B.2.3 The proposed audience and level of interactive engagement with the site, for example whether pupils, school staff or members of the public will be able to contribute content to the site, must be discussed with the school's ICT Manager (or appropriate manager).

B.2.4 Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

B.2.5 The Headteacher or relevant managers must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

B.2.6 There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the school's brand and image.

B.2.7 Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

B3 CHILDREN AND YOUNG PEOPLE

B3.1 When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.

B3.2 When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online "friends" as real friends, be targets for "grooming" or become victims of cyberbullying.

B3.3 If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.

B3.4 Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, 2008)

B3.5 Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

B3.6 Care must be taken to ensure that content is suitable for the target age group and contributors or "friends" to the site are vetted.

B3.7 Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from your ICT Manager or Head teacher.

B4 APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE

B4.1 All Saints Catholic Primary School social media sites can be created only by or on behalf of the school.

Site administrators and moderators must be All Saints Catholic Primary School employees or other authorised people.

B4.2 Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the staff member's line manager, the school's ICT Manager and the headteacher.

B4.3 Approval for participating, on behalf of All Saints Catholic Primary School, on sites created by third parties must be obtained from the staff member's line manager, the school's ICT Manager and ultimately the headteacher.

B4.4 Content contributed to own or third-party hosted sites must be discussed with and approved by the staff member's line manager and the school's ICT Manager and headteacher.

B4.5 The school's ICT Manager and headteacher, must be consulted about the purpose of the proposed site and its content. In addition, the ICT Manager's and headteacher's approval must be obtained for the use of the school logo and brand.

B.4.6 Staff must complete the Social Media Site Creation Approval Form (**Appendix C)** and forward it to the school's ICT Manager and headteacher before site creation.

B4.7 Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Headteacher immediately. Staff members must not communicate with the media without the advice or approval of the Headteacher

B5 CONTENT OF WEBSPACE

B5.1 All Saints Catholic Primary School hosted sites must have clearly expressed and publicised Terms of Use and House Rules. Third-party hosted sites used for work purposes must have Terms of Use and House Rules that conform to the school of professional conduct and service.

B5.2 Staff members must not disclose information, make commitments or engage in activities on behalf of All Saints Catholic Primary School without authorisation.

B5.3 Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school"s image, reputation and services.

B5.4 Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

B5.5 Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

B5.6 Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

B5.7 All Saints Catholic Primary School hosted sites must always include the school logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website.

B5.8 Staff members participating in All Saints Catholic Primary School hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites.

B5.9 Staff members must never give out their personal information such as home contact details or home email addresses on these sites.

B5.10 Personal opinions should not be expressed on official sites.

B6 CONTRIBUTORS AND MODERATION OF CONTENT

B6.1 Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.

B6.2 Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.

B6.3 The content and postings in All Saints Catholic Primary School hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.

B6.4 The Network team must designate at least one member of staff whose role it is to review and moderate the content, including not posting or removal of comments which breach the Terms of Use and House Rules. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.

B6.5 For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention. For example, in the case of content raising child safeguarding concerns or comments likely to cause offence.

B6.6 Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.

B6.7 All Saints Catholic Primary School does not allow any outsiders to become friends of the site and to limit the site to known people only, in the case of adults, those who have undergone appropriate security checks.

B6.8 Any proposal to use social media to advertise for contributors to sites must be approved by the school's ICT Manager and headteacher.

B6.9 Approval must also be obtained from the school's ICT manager and headteacher to make an external organisation a "friend" of the site.

Appendix (C) "Social media creation approval form"

Use of any social media on behalf of All Saints Catholic Primary must be approved prior to setting up sites.

Name of Social Media:

PURPOSE OF SETTING UP SOCIAL MEDIA SITE
(please describe why you want to set up this site and the content of the site)

- What are the aims you propose to achieve by setting up this site?

- What is the proposed content of the site?

- What do you think are the benefits of the site for the school?

PROPOSED AUDIENCE OF THE SITE
(Please highlight all that apply as appropriate)

Pupils of All Saints RC Primary School

Head and School staff

Pupils' family members

Pupils from other schools (provide names of schools)

External organisations

Members of the public

Others; please provide details

PROPOSED CONTRIBUTORS TO THE SITE

Signed: Mr J Price (HT) Mrs P Zagozda (CoG)
Date: Nov 2023