Bishop Vaughan Catholic School

E-Safety Policy

E-Safety Policy

The Church's interest in the Internet is a particular expression of her longstanding interest in the media of social communication. Seeing the media as an outcome of the historical scientific process by which humankind "advances further and further in the discovery of the resources and values contained in the whole of creation", the Church often has declared her conviction that they are, in the words of the Second Vatican Council, "marvellous technical inventions" that already do much to meet human needs and may yet do even more.

From the introduction to *The Church and Internet* (Pontifical Council for Social Communications)

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by an e-safety working group.

- Assistant Headteacher
- Wellbeing Officer
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Pupils

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Dealing with emerging situations and the importance of e-safety

Since the Coronavirus pandemic of 2020, it has been necessary for school staff and pupils to use digital platforms more frequently in order to support continuity of learning during periods of isolation and/or periods of remote learning. In light of this, there has been increased emphasis on training colleagues and pupils so that all stakeholders are appropriately prepared to use these platforms safely and responsibly.

Schedule for Development / Monitoring / Review

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

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.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals 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 Governor's receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor (Mr J Williams). The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / committees / meetings

Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator / Officer.
- The Headteacher and other members of the Senior Leadership Team 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.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher and Senior Leaders 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 will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.
- The Headteacher and Senior Leaders have responsibility for updates to the policy and to deal with emerging situations on the wider educational horizon which require this policy to updates. Any updates should be discussed the Governor with responsibility for E–safety and also presented to the Governing Body for approval.

E-Safety Coordinator / Safeguarding 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 e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of e-safety incidents 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 filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body 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 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 / Senior Leader; E-Safety Coordinator
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

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
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; E-Safety Coordinator for investigation
- 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 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

Child Protection / Safeguarding Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- 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 self-review tool

Students / pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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

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 e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety 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

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.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of 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 Computing / PSE / 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
- 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the 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 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, 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 (e.g. 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:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

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 website will provide e-safety information for the wider community

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:

- **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.**
- **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 / Officer (or other nominated person) will receive regular updates through attendance at external training events
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) 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 / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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 e-safety 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** 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 frequently.
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)**
- The Network Manager **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.
- The school has provided enhanced / differentiated user-level filtering
- 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 users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place 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" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- 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 (e.g. 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.

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 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 e.g. 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.
- 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.
- 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 current data protection legislation.

The school:

- has a Data Protection Policy.
- has implemented the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it. The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- has developed and implemented a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. The school has systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.

- has provided staff, parents, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- has in place Data Protection Impact Assessments (DPIA) that are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- understands how to share data lawfully and safely with other relevant data controllers.
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- ensures all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

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.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- 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

Communications

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:

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

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 (e.g. 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.
- 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

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.

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

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

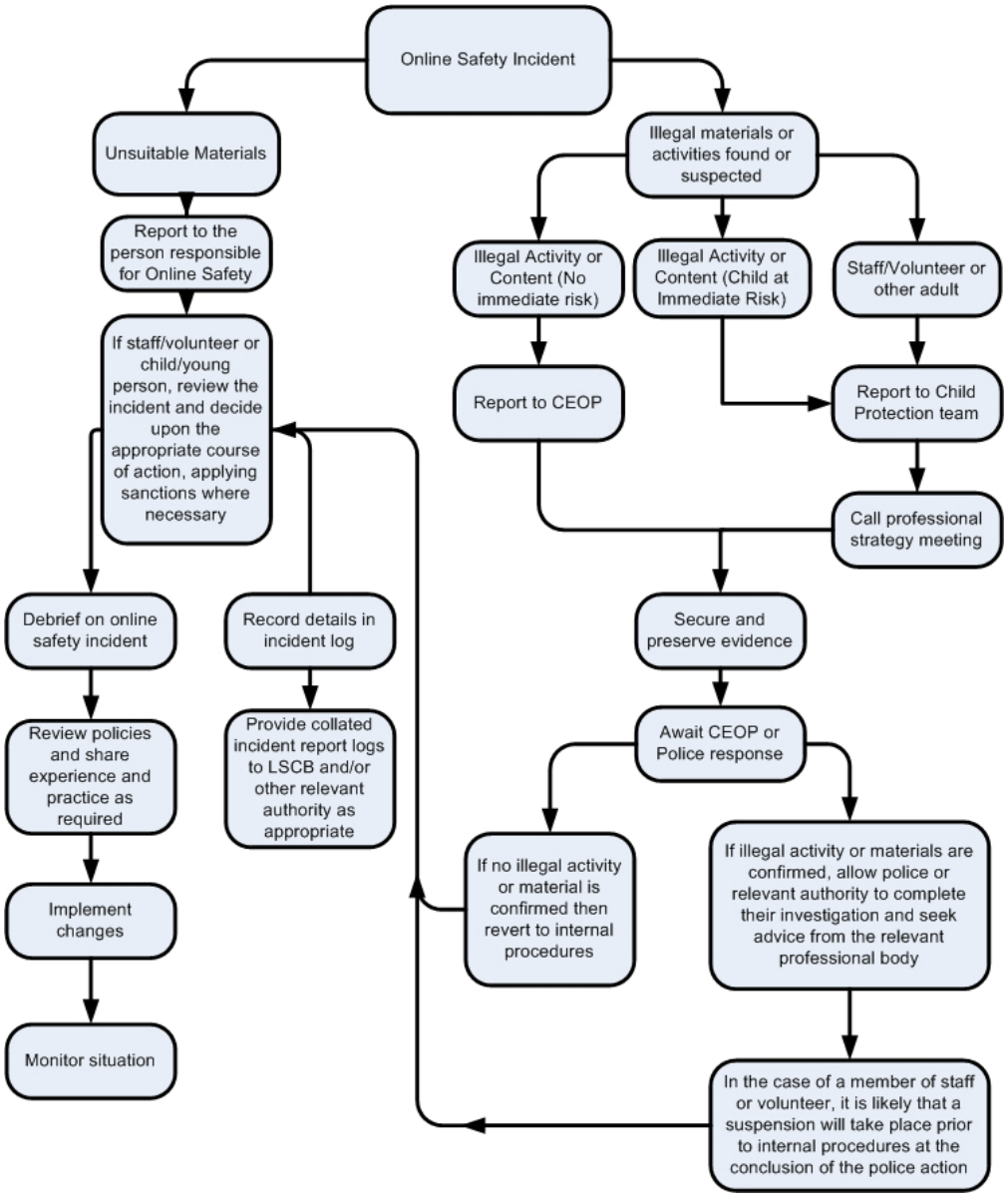
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse 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				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 (e.g. 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 e.g. YouTube			x			

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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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 / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	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 e.g. 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							x
Unauthorised use of social media / messaging apps / personal email		x			x				x
Unauthorised downloading or uploading of files		x			x				x
Allowing others to access school network by sharing username and passwords		x			x				x
Attempting to access or accessing the school network, using another student's / pupil's account		x			x				x
Attempting to access or accessing the school network, using the account of a member of staff		x			x	x			x
Corrupting or destroying the data of other users		x			x	x	x		x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x		x					x
Continued infringements of the above, following previous warnings or sanctions		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		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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x							x	x

Staff Actions / Sanctions

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
Inappropriate personal use of the internet / social media / personal email	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 e.g. holding or transferring data in an insecure manner	x				x	x		
Deliberate actions to breach data protection or network security rules	x	x	x		x			x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x		x			x
Sending an email, text or 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		
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					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			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		x			x

E-safety within the context of the COVID- 19 pandemic and schools using digital platforms for continuity of learning

Since the Coronavirus pandemic of 2020, it has been necessary for school staff and pupils to use digital platforms more frequently in order to support continuity of learning during periods of isolation and/or periods of remote learning. In light of this, there has been increased emphasis on training for school colleagues and pupils so that all stakeholders are appropriately prepared to use these platforms safely and responsibly.

Protocols for interactive sessions to protect staff and safeguard pupils

In recognition of the rapidly changing situation and in striving to strengthen our offer to best serve our learners, the following protocols must be adhered to by stakeholders order to support asynchronous and synchronous learning and to ensure appropriate safeguarding.

Key definitions – Digital platform

The agreed digital platform in school is Microsoft Teams. All staff must use Microsoft Teams as the digital platform to communicate with pupils using a registered Hwb account.

Key definitions - Asynchronous learning

Asynchronous learning refers to pupils learning from materials shared by the teacher at different times. This can take the form of a recorded lesson shared by a teacher or an assignment or discourse across a digital platform.

Key definitions- Synchronous learning

Synchronous learning refers to pupils learning at the same time e.g. through a live session across a digital platform. Types of synchronous lessons in Bishop Vaughan include a 'live teaching session' where teachers share materials visually and interact with students orally. A second type includes an 'interactive' session where the teacher is present at the same time as students to answer and ask questions and interact via the chat box. These sessions are important in providing opportunities for students to access the expertise of their teachers during exceptional times. This support could be vitally important for some pupils when they are preparing for a task, to consolidate their understanding during a task or to dispel a misconception.

For the purpose of clarity, we are in a position as a school to draw subtle differences between

a. **synchronous 'live lessons'** where the **teacher's camera and/ or microphone is switched on** and
b. **synchronous 'interactive sessions'** where the **teacher camera and/ or microphone are switched off.**

For ease of reference, the protocols outlined below apply to both.

All synchronous learning sessions must also adhere to the broader guidance shared by the Local Authority on live streaming which can be found at:

https://swanseavirtualschool.org/wp-content/uploads/2020/10/Live-Streaming-Guidance-v0.6.pdf

The following school protocols are drawn together and it is suggested that the following guidance is read in conjunction with the LA policy on live streaming referred to above.

Preparation for the delivery of synchronous/ interactive sessions at Bishop Vaughan Catholic School

- Staff training has been delivered on synchronous sessions through digital drop ins and buddy systems, live lesson walkthrough to explore the functions (e.g. hands up, the lobby, chat box), Local Authority webinars and through additional training on the clarity of instruction from external partners
- Guidance has been shared with colleagues on synchronous learning in the school's 'Planning for Continuity of Learning Document' and through Blended Learning updates
- A synchronous learning working party has been established to promote staff dialogue, and to provide a forum for the exchange of tips and technical know how
- No member of staff is expected to carry out any online live lesson teaching which makes them feel uncomfortable
- Teams is the agreed platform for interactive sessions – no other platforms are permitted for use
- Class teams have been created to support remote learning across Teams
- Alternative arrangements are in place for students who cannot access synchronous/ interactive sessions
- Through pupil induction arrangements, familiarity on how to use the platforms has increased across the student body
- Rules on acceptable behaviour whilst participating in learning across digital platforms have been shared with pupils

Safeguarding and regulatory protocols

- Any safeguarding concerns arising from an interactive session should be raised directly with Carl Walker or Kirsty Thomas, in adherence to the usual safeguarding procedures
- Colleagues must share clear behaviour rules with pupils prior to the start of synchronous learning as part of the notes in the Teams invitation sent out to pupils and to also share those rules at the start of a session. Generic and simple rules include: pupil cameras off, use the chat function for comments, pupils speak when only invited to by the teacher, use of appropriate language and tone as would be used in the classroom
- The Governing Body will be kept abreast of school policy updates and also any safeguarding issues linked to interactive sessions
- A second member of staff on a synchronous session is always essential
- Staff must use the lobby function to control admittance to a synchronous session
- Where possible session invitations should be sent out to pupils two days prior to the session in order to promote pupil engagement

- Interactive sessions will not be recorded – a second person on the call will be sufficient for safeguarding purposes
- Consent has been sought from pupils to participate in synchronous sessions - a small number of pupils/ parents have withheld consent – staff are required to check the All Staff Teams – Blended Learning – Consent folder for up to date lists. Lists will change over time and frequent checking is needed.
- Only school laptops are permitted for use to deliver interactive sessions
- Only Hwb registered accounts are permitted for use – do not use personal accounts under any circumstances

*****

Copies of this policy are available on our website, in policy folders on the school network and can be made available on request.

Date: June 2017
Reviewed: June 2019
Reviewed: February 2021
Reviewed: February 2023
Policy Next Review Date: February 2025

Annexe A

Staff, Governor and Visitor
ICT Acceptable Use Agreement / Code of Conduct

- I will only use the school's e-mail/Internet/Intranet/Learning Portal and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.

- I will only use the approved, secure e-mail system(s) for any school business.

- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.

- I will not install any hardware or software without the permission of the Network Manager.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal, defamatory or discriminatory.

- Images of pupils and/or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.

- I understand that my use of the Internet and other related technologies may be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

- The above should be seen as the Code of Conduct under ordinary circumstances. Any deviation from this code should be approved by the Headteacher or Senior Leadership Team.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature …… **Date** ……

Full Name ……..... (printed)

Job title . . . . . .

An electronic copy of this form can be signed online