CHRIST THE KING PRIMARY SCHOOL

ONLINE SAFETY

(including acceptable use, internet and mobile technology)

Updated: November 2024

Christ the King Primary School
Everest Avenue
Llanishen
Cardiff
CF14 5AS
Tel: 02920754787
Email:
www.christthekingcathprm.co.uk

Date for Review: January 2026

Development/monitoring/review of this policy

This online safety policy has been developed by:

- Headteacher/SLT
- Digital Lead/ Online Safety Coordinator
- Staff – including teachers/support staff/technical staff
- Governors

Schedule for development/monitoring/review

This online safety policy was approved by the governing body/governors sub-committee on:	Anna Buckland
The implementation of this online safety policy will be monitored by the:	• Headteacher/SLT • Digital Lead • Governors
Monitoring will take place at regular intervals:	Termly
The governing body will receive a report on the implementation of the online safety policy at regular intervals	Yearly

The online 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 online safety or incidents that have taken place. The next anticipated review date will be:	January 2026

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:
    - learners
    - parents and carers

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Online Safety personnel:

Governor: Anna Buckland

Headteacher: Mrs S Miles (DHT Helen Oyston in Head's absence)

Online Safety Coordinator: Mrs Warrington

Online Safety Committee

- Headteacher: S Miles (DHT Helen Oyston in Head's absence)
- Online Safety Coordinator: Mrs Warrington
- Designated person for child protection / Child Protection Officer: Anna Buckland
- Governor: Anna Buckland
- 2 School parliament group members from School Council Online Safety committee, elected annually: TBC

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of online safety governor to include:

- Regular meetings with the online safety officer.
- Regular monitoring of online safety incident logs.
- Reporting to relevant governors/sub-committee/meetings.

Headteacher and senior leaders:

The Headteacher and SLT are responsible for ensuring that:

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to the Online Safety Coordinator.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff**.**
- The headteacher and senior leaders are responsible for ensuring that the digital lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.
- 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 online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The headteacher will receive regular monitoring reports from the Online Safety Coordinator.

Online safety coordinator:

The Online safety coordinator is responsible for ensuring that:

- Leads the online safety group – parliament group tbc.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides (or identifies sources of) training and advice for staff.
- Liaises with the Cardiff Local Authority and Central South Consortium.
- Liaises with technical staff – Cardiff IT Services and iTeach.

- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments – OneDrive
- Meets with online safety governor to discuss current issues, review incident logs.
- Attends relevant meeting/sub-committee of governors
- Reports regularly to headteacher.

Technical staff

The technical staff is responsible for ensuring that:

- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the local authority.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- They keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the network/internet/learning platform/hwb/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher/senior leaders; online safety coordinator for investigation/action/sanction

Teaching and support staff

These individuals are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the staff acceptable use agreement (aua) – Appendix 1.
- They report any suspected misuse or problem to the headteacher/senior leader; online safety coordinator for investigation/action.
- All digital communications with learners/parents and carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Learners understand and follow the online safety and acceptable use agreements.
- Learners 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 learners 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.

Designated senior person

The designated senior person should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online bullying.

Online safety Parliament group

The online safety group provides a group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to classes and the Headteacher.

Members of the online safety group will assist the online safety coordinator with:

- The production of the school online safety events timetable.
- Creating age appropriate SMART resources for classes.
- Leading Online Safety events alongside the Online safety coordinator.

Learners

These individuals:

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement.
- Should 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.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's acceptable use agreements covers their actions out of school.

Parents and carers

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

- Digital and video images taken at school events.
- Access to parents'/carers' sections of the website, learning platform (seesaw) and online learner records.

Community users

Community users who access school systems as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. Appendix 2.

Policy statements

ALN Statement

Christ The King Primary School is committed to providing an inclusive learning environment in line with the Additional Learning Needs and Education Tribunal (Wales) Act 2018 and the ALN Code for Wales 2021. We are dedicated to identifying , assessing and making provision for Additional Learning Needs at the earliest opportunity , working in collaboration with pupils, parents, and relevant professionals. Our approach is based on promoting equity, respecting diversity, and ensuring that all pupils are provided with opportunities to meet success .

Education – learners

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the Christ the King's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum across a range of subjects, (e.g. Science & Technology/ Health & Wellbeing /DCF) and topic areas and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and activities.
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Learners should be helped to understand the need for the learner 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 learners 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 learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents and carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online 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.

Christ the King will therefore seek to provide information and awareness to parents and carers through:

- curriculum activities
- letters, newsletters, web site, learning platform, Hwb
- parents and carers evenings/sessions
- high profile events/campaigns, e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. hwb.wales.gov.uk/ www.saferinternet.org.uk/ www.childnet.com/parents-and-carers

Education – the wider community

Christ the King will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school's learning platform, hwb, website will provide online safety information for the wider community.

Education and training – staff/volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The online safety coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/inset days.
- The online safety coordinator will provide advice/guidance/training to individuals as required.

Training – governors

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

- Attendance at training provided by the local authority/National Governors Association/or other relevant organisation, (e.g. SWGfL)
- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

Christ the King working with iTeach will be responsible for ensuring that the school infrastructure/network is as safe and secure.

- 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 Christ the King's technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Good practice in preventing loss of data from ransomware attacks requires a rigorous and verified back-up routine, including the keeping of copies off-site (OneDrive).
- All Christ the King's networks and system will be protected by secure passwords.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by Miss V Jenkins who will keep an up to date record of users and their usernames.
- Passwords are generated by Hwb using a mixture of uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Records of learner usernames and passwords for Foundation Phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- iTeach 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.

- An agreed system is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school's systems.
- An acceptable user agreement is in place regarding the extent of personal use that users (staff/learners/community users) are allowed on school devices that may be used out of school.

Personal data is securely stored using OneDrive and the school's Teams platform.

Mobile technologies

Mobile technology devices are school owned and include tablets, chrome books/laptops that has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the Christ the King's learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Christ the King's online safety education programme.

A mobile technologies policy has been created (appendix 3)

Children are only permitted to use school owned mobile technologies.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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. Christ the King will inform and educate users about these risks and endeavour reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners 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.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school guidelines 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 learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- Learners' names will not be used anywhere on a website or twitter, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school website and Twitter (appendix 4)

Data protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Christ the King must ensure that:

- It has a Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so.

- It 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.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where, why and which member of staff has responsibility for managing it.
- The information asset register lists the lawful basis for processing personal data (including, where relevant, consent).
- 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.
- Data held must be accurate and up to date where this is necessary for the purpose you hold it for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- Data protection impact assessments (dpia) 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.
- 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
- It has undertaken appropriate due diligence and has GDPR compliant contracts in place with any data processors. (Appendix 5 & 6)
- There are clear and understood policies and routines for the deletion and disposal of data.
- It reports any breeches within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law.
- 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.

When personal data is stored on any mobile device the:

- Data must be saved using OneDrive.
- Device must be password protected.
- Device must be protected by up to date virus and malware checking software.
- Data must be securely deleted from the device,

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.
- Will not transfer any school personal data to personal devices.
- 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 OneDrive and secure password protected devices.

Communication technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Christ the King currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults				Learners			
	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	■							■
Use of mobile phones in lessons				■				■
Use of mobile phones in social time	■							■
Taking photos on mobile phones/cameras				■				■
Use of other mobile devices, e.g. tablets, gaming devices	■							■
Use of personal e-mail addresses in school, or on school network	■							■
Use of school e-mail for personal e-mails		■					■	
Use of messaging apps		■						■
Use of social media		■						■

When using communication technologies Christ the King considers the following as good practice:

- The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored.
- Any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform, etc.) Must be professional in tone and content.
- All learners will be provided with individual school e-mail addresses for educational use.
- Learners should be taught about online 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's website and only official e-mail addresses should be used to identify members of staff.

Social media

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 learners, 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 learners 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, bully online, 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 learners and their families and for colleagues and the learning setting.

Christ the King provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- Ensuring that personal information is not published.
- Training being provided including acceptable use, social media risks, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

Christ the King staff should ensure that:

- No reference should be made in social media to learners, parents and 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.

When official school social media accounts are established there should be:

- A process for approval by senior leaders.
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- Christ the King permits reasonable and appropriate access to private social media sites at appropriate times.

Monitoring of public social media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- Christ the King should effectively respond to social media comments made by others according to a defined policy or process.

Christ the King's use of social media for professional purposes will be checked regularly by a senior leader and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Unsuitable/inappropriate activities

Some internet activity such as accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities such as online 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.

Christ the King 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, or out of, 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,	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

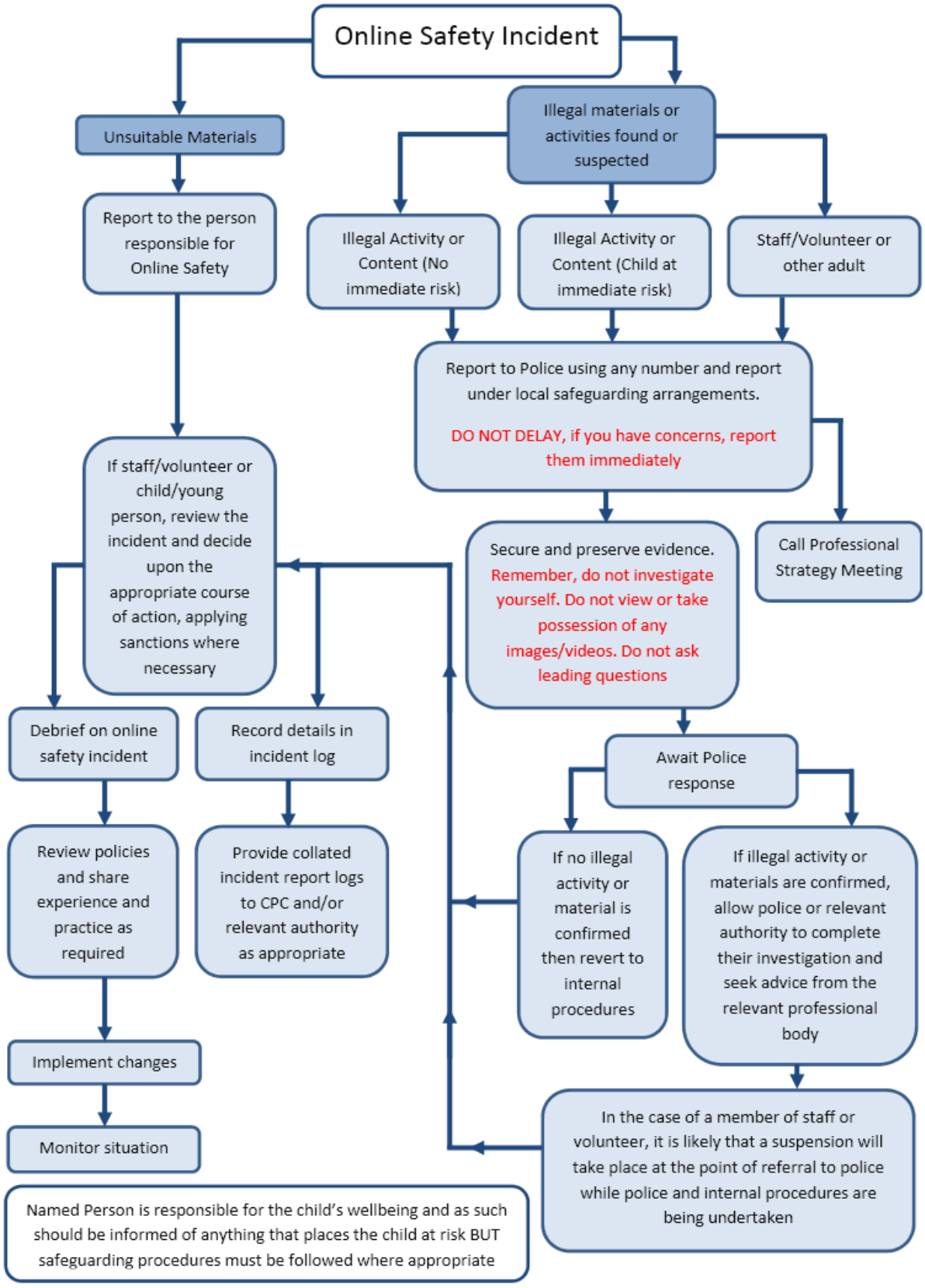
proposals or comments that contain or relate to:	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred 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
	promotion of extremism or terrorism					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, (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	
Online gaming (educational)			X			
Online gaming (non educational)					X	
Online gambling					X	
Online 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 website(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) for responding to online safety incidents and report immediately to the police.



Other incidents:

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:

Learner actions

Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority	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 e-mail		X				X		X
Unauthorised downloading or uploading of files.	X	X			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	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X	X		X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.		X		X		X	X	X
Using personal email/social networking/messaging to carrying out digital communications with learners.	X	X				X		
Actions which could compromise the staff member's professional standing		X	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	X	X				X		X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident.		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations.		X	X		X	X		
Continued infringements of the above, following previous warnings or sanctions.		X	X	X		X	X	X

Appendix 1

Christ the King Catholic
Primary School

Acceptable Use Agreement:
Staff

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users have an entitlement to safe internet access at **all** times.

This Acceptable Use Agreement is intended to ensure that:

- You responsibly stay safe while online ensuring that you are a good role model for younger users.
- Effective systems are in place in school (Firewalls and Equipment Policies) for the online safety of all users and the security of devices, systems, images, personal devices and data.
- You aware of and can protect yourself from potential risk while using online technologies.

Christ the King School will try to ensure that staff and volunteers will have good access to digital technologies to enhance learning opportunities and will, in return, expect staff to agree to be responsible users.

Acceptable use agreement

I understand that I must use Christ the King School's digital technologies in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technologies. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety, I understand that:

- I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring the school into disrepute.
- My use of technology will be monitored.
- When communicating professionally I will use the technology provided by school (e.g. School provided email via HWB).
- These rules also apply when using the school's technology either at home (laptops/iPads) or
- away from the school site.
- Personal use of school technology is only acceptable with permission.

- The use of personal social media profiles to discuss or disseminate any school information is prohibited under this agreement.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it

For the safety of others:

- I will not access, copy, remove or otherwise alter any other user's files, without authorisation.
- I will communicate with others in a professional manner.
- I will only communicate with learners and parents/carers using official school systems (Hwb emails, Google Classrooms and Seesaw). Any such communication will be professional in tone and manner.
- I will share other's personal data only with their permission.
- I understand that any images I publish will be with the owner's permission and follow the school's code of practice, and be in line with latest GDPR and Data Protection Policy.
- I will only use school equipment to record any digital and video images.
- Use of my own equipment to record children or school images is prohibited.

For the safety of the school, I understand that:

- I will not try to access anything illegal, harmful or inappropriate.
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident to the Headteacher.
- I will not share my online personal information (eg social networking profiles) with the children and young people in my care.
- I will not deliberately bypass any systems designed to keep school safe.
- I will only transport, hold, disclose or share personal information about myself or others in line with GDPR. Where personal data leaves the school site, it must be stored using OneDrive.
- I understand that data protection policy and latest GDPR require that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by a school policy to disclose such information to an appropriate authority.
- Personal passwords and those of other users should always be confidential.
- I will not download anything that I do not have the right to use.
- I will inform the Digital Lead and Headteacher if I find any damage or faults with technology.
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use Christ the King School's digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name

Signed

Date

Appendix 2

Christ the King Catholic Primary School

Acceptable Use Agreement: Community Users

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users have an entitlement to safe internet access at **all** times.

This acceptable use agreement is intended to ensure:

- That community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- That school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That users are protected from potential risk in their use of these systems and devices.

Acceptable use agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices.

I have read and understand the above and agree to use the school digital technology systems and my own devices within these guidelines.

Name ..... Signed ..... Date: .....

Appendix 3

Christ the King Catholic Primary School

Mobile Technologies Policy

Mobile technology devices are school owned and include tablets, chrome books/laptops that has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the Christ the King's learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Christ the King's online safety education programme.

The key to considering the use of mobile technologies is that the learners, 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 is school owned or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use agreement, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential benefits of mobile technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high-tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to Christ the King's network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the Christ the King embarked on this path, the risks and benefits have been clearly identified and shared with all stakeholders.

- Christ the King, Cardiff Council and iTeach has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.

- For all mobile technologies, filtering will be applied to the school internet connection and attempts to bypass this are not permitted.
- Mobile technologies must only be used in accordance with the law.
- Mobile technologies are not permitted to be used in certain areas within the school site such as toilets.
- Learners will be educated in the safe and appropriate use of mobile technologies as part of the online safety curriculum
- The school Acceptable Use Agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies.
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users		Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**		No	Yes	Yes
Full network access	*Yes*	*Yes*		No	No	No
Internet only				No	Yes	yes
No network access				No	No	No

School devices

- All school devices are controlled through the use of mobile device management (MDM) software.
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g internet only access, network access allowed, shared folder network access)
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain their property and will not be accessible to learners on authorised devices once they leave the school roll.
- The school is responsible for keeping devices up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
- Christ the King's devices are provided to support learning.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended is not permitted.
- All school devices are subject to routine monitoring.

Personal devices

For staff only:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of filtered network access.
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user as does the liability for any loss or damage resulting from the use of the device in the school.
- Staff personal devices should not be used to contact learners or their families, nor should they be used to take images of learners.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

User behaviour

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school.
- Devices must be in silent mode on the school site.
- Learners must only photograph people with their permission and must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.
- Devices may be used in lessons in accordance with teacher direction.
- Staff owned devices should not be used for personal purposes during teaching sessions, except in emergency situations.

Visitors

Visitors should be provided with information about how, where and when they are permitted to use mobile technology on the site, in line with local safeguarding arrangements. They should also be informed about the school's policy on taking images.

Appendix 4

Christ the King Catholic Primary

Pupil Image Consent Form

Online Safety and Photographic Images

As part of the school's Online Safety policy we adhere to the following guidelines when publishing images of pupils:
· No photographic images will be published without parental consent
· No child's name will be linked to photographic images
· No individual photographic images of children will be used

School Website

The school has its own website https://www.christthekingcathprm.co.uk/

The school regularly updates and develops the content on the website. One part of portraying the school and its good practise is the inclusion of examples of pupils work and photographic images of activities.

The Headteacher and Senior Leadership Team are responsible for ensuring that the content of the school website is accurate and appropriate.

Twitter

The school has a twitter account ctkprmcardiff which is used to celebrate and share the successes of its pupils and to raise the profile of the school within the community and beyond. No photographic images of pupils or their work will be published without parental consent and no names will be linked to the images used.

School Newsletter

The school publishes a termly newsletter highlighting the many activities and events the children have undertaken during the term.

Multimedia Presentations

Multimedia presentations are often included in school assemblies and concerts. By their nature these presentation can include photographic images and videos of pupils.

School Displays

The school learning environment includes displays of pupils work. These can include photographic images of pupils.

Whole Class Photographs

Annually whole class photographs are commissioned from a photographic company.

We kindly request that any photographic images taken or video is not uploaded to social media.

I give consent for my child's image to be published on the following:

☐ Social Media (X, Facebook)

☐ School Publications (School website, newsletter, multimedia presentations and school displays)

☐ Whole class photograph images

I do not give consent for my child's image to be published on the following:

☐ Social Media (X)

☐ School Publications (School website, newsletter, multimedia presentations and school displays)

☐ Whole class photograph images

Please note that you can withdraw consent at any time throughout your child's time at our school. To do so please contact christthekingprm@cardiff.gov.uk

Pupil's Name:	
Parent /Carer's Name:	
Parent/Carer's Signature:	
Date :	

PLEASE RETURN THE SIGNED FORM TO SCHOOL - THANK YOU

Appendix 5

Christ the King Catholic Primary

Hwb GDPR Consent Form

September 2022

Dear Parents/ Guardians,

Please see the information below from Welsh Government. This is a form that requires your consent for then use of Hwb. Hwb is an online platform that the children use in school and can be accessed at home.

For more information about the Hwb platform and how information about your child is used please see https://hwb.gov.wales/privacy

Many thanks

S.Miles
Headteacher

Consent for to allow learners access to additional services

The Hwb platform

The Hwb platform provides all maintained schools in Wales with access to a wide range of centrally funded, bilingual digital tools and resources to support the digital transformation of classroom practices. The Hwb platform is managed and operated by the Welsh Government.

All pupils in maintained schools in Wales must be provided with a secure log-in to the Hwb platform. This is because mandatory reading and numeracy tests, currently on paper, will be moving online and must be completed by each pupil via the platform. In order to provide [you / your child] with a secure log-in, the school will be sending basic information to the Welsh Government. The log-in will allow [you/your child] to take the mandatory online assessments, known as 'personalised assessments'.

For more information about the Hwb platform and how information about [you / your child] is used, please see https://hwb.gov.wales/privacy. For more information about the online personalised assessments, please see http://learning.gov.wales/resources/collections/national-reading-and-numeracytests?lang=en#collection-2

Additional services

If you agree, Welsh Government can also provide [you/your child] with access, via the Hwb platform, to a variety of additional services which are provided by other organisations.
These include online learning environments such as Hwb Classes, Microsoft Office 365, Google for Education, and other relevant educational tools and resources. Welsh Government is making these additional services available to help [you/your child] access educational resources. These additional services are centrally funded and there is no cost for you or for your school to access and use them.

Welsh Government will only provide access to these additional services if you sign the form below to indicate your agreement.

Your agreement
If you agree:

· We will tell Welsh Government to provide access to the additional services

· Welsh Government will share information about [you/your child] with its service provides, including Microsoft and Google Education, in order to enable access to the additional services

If you do not agree, we will still share information about [you/your child] with Welsh Government to set up a secure log-in for the Hwb platform, but [you/your child] will not be able to access the additional services.

If you wish to withdraw your consent, please contact the head teacher within your Christ the King Catholic Primary school.

Please sign and date this form if you agree to the above.

Child's Name ……..

Parents Name in Full ……

Signed ……

Dated …….

Appendix 6

Christ the King Catholic Primary

Seesaw GDPR Consent Form

Dear Parents:

I am delighted to share with you that this school year our class will be using Seesaw (http://seesaw.me), a secure online journal where students can document and reflect on what they are learning in class. Your child will be able to add the things we work on (including photos, videos, worksheets, drawings and voice recordings) to their Seesaw journal and we can share them privately with you and other family members to view and comment on throughout the school year.

In order for your child to use Seesaw, the app needs your child's name in order to be able to associate work like their photos, videos or voice recordings with their account. Seesaw only uses this information to provide the service and doesn't advertise in Seesaw, create profiles of students, or share or sell your child's personal information or journal content. You can read more about their strong privacy promises here: https://web.seesaw.me/privacy.

Under an EU law called the General Data Protection Regulation (GDPR), in order for your child to use Seesaw, the school must get your consent. For more information on GDPR, please visit https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens.

I hope that your child will enjoy using Seesaw to document and share their learning this year. Please sign below and return this permission slip so that your child can use Seesaw.

———————————————————————————————

Please sign below and return the form.

I give consent for my child, listed below, to use Seesaw for class activities.

Student Name: _____

Parent Printed Name: _____

Parent Signature: _____ Date: _____