Online Presence and Internet-enabled Devices Policy

At The Cathedral Catholic Primary School we are safe and cared for; we make Christ known and loved, using his example to strive for excellence in all we do.

In close partnership with parents and the parish of The Cathedral and St Thomas More, we aim to deliver an outstanding and distinctive Catholic education with Christ at its heart. Each person's unique value is recognised and nurtured so that, through God's grace we can grow, learn and realise our full potential.

We use our gifts and talents for the glory of God and in the loving service of others, proclaiming the Gospel and striving for the values of the Kingdom of God.

We profess our faith proudly and recognise that we are called to a loving relationship with God through the sacraments, scripture and prayer.

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will be monitored by the:	*Headteacher, Deputy Headteacher & Computing subject lead teacher*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body will receive a report on the implementation of the Online Presence and Internet-enabled Devices Policy (including anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online Presence and Internet-enabled Devices 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:	*May 2025*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Headteacher (DSL), Deputy Headteacher (DSL) & Computing subject lead teacher, LADO, Police*

INDEX

1. Rationale - The Importance of Internet use in Primary Education

The Internet is ubiquitous, necessary and a fundamental component of an ever interconnected world with significant educational benefits resulting from appropriate curriculum Internet use. An online presence also provides a vital digital dialogue with our parents, wider school family and community partners.

The school has a duty to provide students with quality Internet access as part of their learning experience**.**

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The following Online Presence and Internet-enabled Devices Policy includes all digital devices and platforms, including all Internet-enabled hand-held devices.

Using the Internet in education allows:

- Access to all age-appropriate world-wide educational resources.
- Access to expert up to date knowledge for both pupils and staff
- Communication links to support services, professional associations and colleagues
- Necessary exchange of data with the LGfL and DfES.

Internet use will enhance learning because:

- Use of the Internet will be built into Curriculum Planning for all subjects to specifically enrich and extend the learning process.
- Staff will guide pupils in on-line activities that are planned to support the learning outcomes for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval; appraisal of bias and subjectivity and copyright materials.

2. Scope of this policy

This policy applies to all members of Cathedral's community (including staff, pupils, volunteers, parents / carers, visitors, and community users) who have access to and are users of school digital technology 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. This is pertinent to incidents of online-bullying or other Online 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.

3. Overview of Issues and Risks

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Digital technologies can offer many positive educational and social benefits to both adults and pupils, and both should be clearly educated on the benefits and risks involved when going online, including:

- **Copyright infringement** - Copyright law applies on the Internet: staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

- **Exposure to inappropriate materials** - There is a risk that when using the Internet, young people may be exposed to material that is pornographic, hateful and violent in nature, encourages activities that are dangerous or illegal, is just age-inappropriate, biased or in contrast to Cathedral's whole-school values. Cathedral seeks to build pupil's understanding and confidence in dealing with e-Safety issues, both at home and school.

- **Inappropriate or illegal behaviour** - Online bullying is an unfortunate aspect of the use of Internet-enabled technologies. This can damage victim's self-esteem and pose a threat to their wellbeing. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:
    - No access to chat-rooms, Instant Messaging services, Social Media platforms and bulletin boards.
    - Pupils are taught how to use the Internet safely and responsibly in line with our Safeguarding, PSHEE, Computing policies and Keeping Children Safe in Education (September 2021).

- **Sexual Harassment, Online Sexual Abuse and Sexual Violence** Sexual violence and sexual harassment can occur between two children of any age and sex from primary through to secondary stage and into colleges. It can occur through a group of children sexually assaulting or sexually harassing a single child or group of children. Sexual violence and sexual harassment exist on a continuum and may overlap; they can occur online and face to face (both physically and verbally) and are never acceptable.

- **Physical danger and sexual abuse** - Criminal minorities make use of the Internet to make contact with young people with the intention of establishing and developing relationships with young people with the sole purpose of persuading them into sexual activity. There is also a risk that while online a young person might provide information that can personally identify them or others, or arrange to meet people they have met online, so posing a risk to their safety or that of their family or friends.

- **Inappropriate or illegal behaviour by school staff** - This may include viewing or circulating inappropriate material via email, or much more serious activities such as viewing, possessing, making or distributing indecent images. Inappropriate activity by a staff member may result in a disciplinary response by the school or authorities.

4. Principles of Internet Safety

The School Internet Policy is built on the following five core principles:

Guided educational use - Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. There is a clear distinction of learning ***about*** Computing & Digital Technologies and learning ***with*** computing & digital technologies.

Risk assessment – Use of the Internet poses certain risks to which our pupils are aware and able to act responsibly. We will ensure that everyone is fully aware of such risks, perform risk assessments

and implement the policy for Internet use. Pupils need to know how to act and report inappropriate material.

Responsibility - Internet safety depends on staff, schools, governors, advisers, parents and the pupils themselves taking responsibility for the use of Internet on all devices. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions will be judged carefully.

Regulation - The use of unsuitable resources, for instance un-moderated chat rooms or Instant messaging services present immediate dangers that are challenging to monitor and are therefore banned.

Appropriate strategies - This policy describes a number of strategies to help to ensure responsible and safe use. They include developing children's 'netiquette' in response to safe and responsible Internet use, developing responsibility and on guiding pupils towards educational activities. This requires staff, parents and pupils to be active participants and supporters of safe online activities

5. Creating a safe E-learning environment

A foundation for creating a safe Computing learning environment is to ensure that everyone is aware of online and digital profile and how this may impact upon the school environment and the pupils. Awareness will be raised, in part, by a comprehensive Internet safety education programme for the whole school community.

5.1 Roles and responsibilities

Internet Safety Co-ordinator

- The primary responsibility of the Internet Safety Co-ordinator (Computing & Digital technologies Subject Lead Teacher) will be to establish a safe Computing learning environment within the school.
- Ensuring that any incidents in which Internet safety is breached are responded to in an appropriate and consistent manner, with the appropriate authority to take action as necessary.
- Leading in the creation of a staff professional development programme that addresses both the benefits and risks of Internet-enabled technologies.
- Leading in the creation of an Internet safety education programme for pupils, maintaining an overview of activities across the school, and supporting staff with information and resources as appropriate.
- Developing a parental awareness programme.
- Maintaining a log of all incidents relating to Internet safety in school.
- Updating the governing body on current Internet safety issues, in conjunction with the Headteacher.
- Liaising with outside agencies, which may include the LEA, local schools, or national agencies, as appropriate.

Headteacher

- Taking ultimate responsibility for Internet safety issues within the school, while delegating day-to-day responsibility to the Internet Safety Co-ordinator.
- Supporting the Internet Safety Co-ordinator in creating an Internet safety culture within the school, including speaking to staff and pupils in support of the programme
- Ensuring that the Governing body is informed of the issues and the policies

- Ensuring that appropriate funding is allocated to support Internet safety activities throughout the school, for both the technical infrastructure and Inset training promoting Internet safety across the curriculum.

Governing body

- The Governing body has statutory responsibilities for child protection and health and safety, and elements of these will include Internet safety.
- Developing an understanding of existing school policies, systems and procedures for maintaining a safe Computing learning environment and supporting the Headteacher and E-safety Co-ordinator in implementing these, including ensuring access to relevant training for all school staff
- Promoting Internet safety to parents, and providing updates on Internet safety policies.

Teaching Staff and Volunteers

- Develop and maintain knowledge of Internet safety issues, particularly with regard to how they might affect children and young people
- Implementing school policies through effective classroom practice
- Ensuring any instances of computer misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the Internet Safety Co-ordinator in line with school Internet safety policies
- Planning classroom use of the Internet and computing facilities to ensure that Internet safety is not compromised; for example, evaluating websites in advance of classroom use (for example, by bookmarking and caching sites) and ensuring that school filtering levels provide appropriate protection for topics being studied
- Embedding teaching of Internet safety messages within curriculum areas wherever possible (i.e. PSHE and Computing Policy)
- Maintaining an appropriate level of professional conduct in their own Internet use both within and outside school (see Social Media - Protecting Professional Identity)

Pupils

- Upholding school policies relating to acceptable use of the Internet and other communications technologies
- Developing their own set of safe and discriminating behaviours to guide them whenever they are online
- Reporting any incidents of Computing & Digital technology misuse within school to a member of the teaching staff
- Seeking help or advice from a teacher or trusted adult if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way
- Communicating with their parents or carers about Internet safety issues, and upholding any rules for safe Internet use in the home

5.2 Technological tools

- The school will work in partnership with the LEA to ensure systems are in place to protect pupils and that they are reviewed and improved.
- An LEA filtering system is in place to minimise access to inappropriate content via the school network.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the LEA via the e-safety co-ordinator.
- It will be possible to keep track of web pages visited and downloaded files to help investigate possible issues and monitor Internet usage.

5.3 Internet safety education programme for the whole school community

Pupils

It is crucial to teach pupils how to use the Internet safely as well as educated about the potential risks of having an online presence, both at school and at home. Clearly however, Internet and computing technologies literacy is unfortunately not synonymous with Internet and computing safety.

- The school will ensure age-appropriate information technology and digital fluency skills are embedded in the heart of the curriculum.
- Safe-surfing messages should be reinforced every time pupils use the Internet and related technologies.
- Instruction in responsible and safe use should precede Internet access.
- 'Rules of Internet use' will be posted in all areas of use. Pupils will be reminded of their acceptance of the rules and related consequences should the rules be breached.
- Pupils will be informed that Internet use will be monitored.
- Pupils should be taught to be critically aware of the materials they read and know that material is not necessarily valid just because it is on the Internet.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- The Computing Curriculum includes a termly focus on Internet safety: Autumn 2 Purple Mash unit of work for all years, Spring term Safer Internet Day activities (Feb) and a whole school theme day in Summer 2 to support children over the summer break.

Parents

Parents and carers also have a key role to play in partnership with the school to create a safe online learning environment and culture, through promoting Internet safety at home, which reinforce the messages taught in school. In this way, we can promote responsible and safe Internet use at home and in school.

- E-safety meetings for parents are arranged on a regular basis. These meetings are available for both parents and children to attend.
- Parents' attention will be drawn to the Online Presence and Internet-enabled Devices policy in newsletters, the school prospectus and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Sign-posting parents & carers to online support resources (See References & Resources)

5.3.1 Sexual Harassment, Online Sexual Abuse and Sexual Violence

- Sexual violence and sexual harassment can occur between two children of any age and sex, from primary through to secondary stage and into colleges. It can occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

- Sexual violence and sexual harassment exist on a continuum and may overlap; they can occur online and face to face (both physically and verbally) and are never acceptable. all staff working with children are advised to maintain an attitude of 'it could happen here'.

- Addressing inappropriate behaviour (even if it appears to be relatively innocuous) an be an important intervention that helps prevent problematic, abusive and/or violent behaviour in the future.

Paragraph 23 (page 14) of **Sexual violence and sexual harassment between children in schools and colleges: Advice for governing bodies, proprietors headteachers, principals, senior leadership teams and designated safeguarding leads (September 2022) states:** *Schools and colleges have a statutory duty to safeguard and promote the welfare of the children at their school/college***.**

Further, paragraph 39 (page 18) states: *The role of education in prevention. Schools and colleges can play an important role in preventative education. Keeping children safe in education sets out that all schools and colleges should ensure children are taught about safeguarding, including how to stay safe online. Schools should consider this as part of providing a broad and balanced curriculum.*

This is directly identified through the school's **Internet safety education programme for the whole school community** (see 5.3) and managed by **13 Responding to incidents and reports** (see below).

5.4 E-mail Management

- Pupil access to e-mail in the school is via Purple Mash only. Class e-mails are available and in certain supervised projects and lessons a pupil's individual account can be created. Pupil's individual accounts will only be available for the duration of the project and should not last for longer than one academic year, where passwords will be reset by the account manager.
- Staff should not use school computing facilities to access external personal e-mail accounts for business unrelated to their professional roles.
- A responsible adult will supervise pupils when writing and sending e-mails and the content of outgoing and incoming e-mails should be checked by the adult (the class teacher whenever possible). This should lessen the risk of inappropriate materials being exchanged.
- Children will be taught to never reveal personal details such as home addresses or telephone numbers during e-mail dialogue
- Pupils will be taught to write polite and responsible e-mails.
- The class teacher has responsibility to ensure that no abuse of the e-mail facility occurs
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

5.5 Newsgroups, Chat Rooms and Instant Messaging

- Pupils will not be allowed access to public or unregulated chat rooms, newsgroups or instant messaging services.

5.6 Managing Internet use

- Pupil's mobile phones or other internet enabled devices are not permitted in school apart from Year 6 (see Mobile Phone Use).
- These devices will:
    - Be kept powered off during the school day
    - Collected and stored by the class teacher
    - Brought in to school at the owner's risk

6. Web site content management

The school has a school website for the purpose of:

- Keeping parents informed about important, dates and events
- Providing information about the school and its related policies.
- Celebrating success and promoting Cathedral's whole-school values and pupil voice

The following non-negotiables must be adhered to:

- Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- Image files will be appropriately named (pupils names not used in image file names) and are appropriately stored on the school's network.
- Image use will be in accordance with the school's photo permission policy.
- The Headteacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.

- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

7. Safe and appropriate management of digital images

The school has given consideration to the way in which digital images including video are captured and stored within school for the protection of both pupils and staff. There are a number of internet-enabled hand held-devices with digital photography capabilities. Staff are made aware of the appropriateness of holding images on personal digital cameras and video. Pupils may also be involved in video conferencing activities where there is the possibility of images captured by a 3rd party.

- Images will be taken and stored on school equipment only – as outlined in the school's Child Protection policy.
- Images captured on digital devices will be transferred to the school server immediately (where practicable) and cleared off devices immediately (where practicable) – this is also to aid management of digital devices
- If images are taken with personal equipment they should be transferred to the school network as soon as possible and deleted immediately.
- Images of pupils or staff will not be captured or copied without permission and will not be stored at home without permission
- All images and video where possible should be stored on the secure TEACHERS shared drive area of the network and files clearly named for ease of archiving material.

8. Internet access authorisation

- The school will keep a record of all staff, pupils and 3rd parties who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Written permission from parents or carers will be obtained before any type of Internet access is allowed.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials such as the use of bookmarked sites or web quests, where pre-tested and approved sites only are accessible. This provides a good model for Internet access at lower Key Stage 2 although the range of sites available may increase.
- Pupils in upper Key Stage 2 may, under supervision, use search engines to carry out approved searches. Searches using 'child friendly' search engines such as 'Ask Jeeves for Kids' and 'Yahooligans' is recommended. Free Internet searching is highly discouraged – teachers should assess the potential risk before undertaking such activity.
- Staff should not conduct free searches using classroom presentation equipment in full view of pupils. Screens should be turned off or frozen whilst staff check suitability of search results.
- Pupils may not use the Internet at any time without supervision. They should be reminded of the rules for Internet use at regular intervals.

9. Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes our Online Presence and Internet-enabled Devices Policy sets out clear guidance for all staff, volunteers and Governors to manage risk and behaviour online.

At its core is the protection of pupils, the school and the individual when publishing any materials online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'.

School staff, volunteers and Governors should ensure that:

- No reference should be made in social media to pupils, parents/carers or school and 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

9.1 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 the school 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. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

10. Mobile Phones in School

The Mobile Phones in School Policy (as part of this Online Presence and Internet-enabled Devices Policy) applies to all pupils and adults during school hours on the school site. Mobile phones are not permitted on school trips or residential visits.

10.1 Responsibility

- It is the responsibility of staff and pupils who bring mobile phones to school to abide by the guidelines outlined in this document.
- The decision to provide a mobile phone to their children should be made by parents or guardians. Parents should be aware that their child takes a mobile phone to school. The mobile phone will be kept by the class teacher in a box in the classroom. This request is only available for Year 6 children.

10.2 Pupils

Pupils are discouraged from bringing phones to school however in Year 6 pupils are permitted to bring communication and hand-held internet enabled devices (these may include phones, kindles, small tablets and MP3 players). It is acknowledged that providing a child with a mobile phone gives parents reassurance that the child can contact a parent if they need to speak to them urgently on their way to or from school. The school also wishes to prepare Year 6 pupils for their transition to secondary school.

- If pupils bring a mobile phone to school, the phones must be switched off while pupils are in class, the school building and the school grounds.

- Pupils should mark their mobile phones clearly with their name.
- Pupils who bring a mobile phone to school should NEVER leave it in their coat/bag when they arrive. To reduce the risk of damage or theft during school hours, mobile phones will be collected by the class teacher and locked securely away.
- The school accepts no responsibility for replacing lost, stolen or damaged stolen phones.
- The school accepts no responsibility for pupils who lose or have their mobile phones stolen while travelling to and from school.
- Any mobile phones seen on the school premises being used at an inappropriate time will be confiscated immediately by a member of staff until the end of the day. At this time, it will be the responsibility of the parents to collect the phone from school, NOT the pupils. If a pupil is found taking photographs or video with a mobile phone of anyone, this will be regarded as a serious offence and disciplinary action will be taken.
- Pupils are advised not to use their mobile phones as they walk to school, unless there is an emergency, as there have been traffic incidents involving pupils who are texting or talking on the phone and not paying full attention to their road use.

10.3 Adults

These instructions apply to any adults with a mobile phone on site, including, staff, volunteers, parents and visitors:

- Practitioners are permitted to have their mobile phones about their person: however there is a clear expectation that all personal use is limited to allocated lunch and/or tea breaks.
- Other than in agreed exceptional circumstances, phones must be switched off/or put on silent and calls and texts must not be taken or made during work time.

- It is acknowledged that there are some circumstances when personal devices like mobile phones maybe used to take and record images in school (eg school trips, visitors, celebration days etc). If practitioners use their phones for taking and recording images, the following guidelines should be followed in line with **7. Safe and appropriate management of digital images** (see above) :
    - Images captured on digital devices will be transferred to the school server immediately (where practicable) and ***cleared off*** devices immediately (where practicable) – this is also to aid management of digital devices
    - If images are taken with personal equipment they should be transferred to the school network as soon as possible and ***deleted*** immediately.

- Practitioners are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting, in a professional capacity.
- Parents, visitors and contractors are respectfully requested not to use their mobile phones in any of the designated mobile free areas. Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by children in order to avoid any unnecessary disturbance or disruption to others.
- On off-site trips, including residentials, all accompanying adult helpers are permitted to have their mobile phones, but use is limited to agreed off duty times and away from the children.
- Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.
- Any breach of these procedures could lead to the Headteacher and governing body being informed and consequently disciplinary action according to the school's procedures.

11 Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR) announced in 2016. As a result, The Cathedral may be subject to greater scrutiny in our care and use of personal data

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

We will ensure that:

- There is a clear Data Protection Policy.
- A Data Protection Officer (DPO) has been appointed.
- Minimum personal data will be held and only necessary to enable the school 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. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- There are clear arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures are in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- The school has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

11.1 Staff must ensure that they:

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

11.2 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 once it has been transferred or its use is complete.

12. Staff consultation

- All staff must accept and sign the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the Online Presence and Internet-enabled Devices Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required.

13. Responding to incidents and reports

Minor incidents

- Minor incidents of misuse by pupils might include; copying information into work and failing to acknowledge the source, downloading materials or images not relevant to their studies, and misconduct associated with pupils files, such as using someone else's password or deleting someone else's files.
- The Internet Safety Co-ordinator will monitor minor incidents to identify trends in pupils' behaviour, and will react to any emerging issues. This might include raising awareness on a particular Internet safety topic at a school assembly or offering staff additional training.

Incidents involving inappropriate materials or activities

- Specific breaches of policy and rules might include deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network.
- Serious incidents relating to Internet safety in schools will be reported to the Internet Safety Co-ordinator immediately. The Internet Safety Co-ordinator must document the incident and decide on an appropriate course of action, which will include involving the Headteacher and may also include external agencies. It may also be necessary to involve child protection
- Staff to provide follow-up counselling and support .
- The Internet Safety Co-ordinator will review Internet safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.
- If a child discovers something on the Internet that makes them feel uncomfortable or upset, they must report it immediately to their teacher. Pupils will be taught to turn off the monitor so that attention is not drawn to the material.
- Although the Internet access at Cathedral is filtered in order to screen inappropriate sites, it may still contain inappropriate material. The site must be reported immediately to the Internet Safety Co-ordinator who will ensure that the website is flagged county-wide.

Incidents involving illegal materials or activities

- Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the Headteacher, then ultimately the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on

or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched. Under no circumstances should the Internet Safety Co-ordinator, network manager or Headteacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

Reports of Sexual Harassment or Sexual Violence

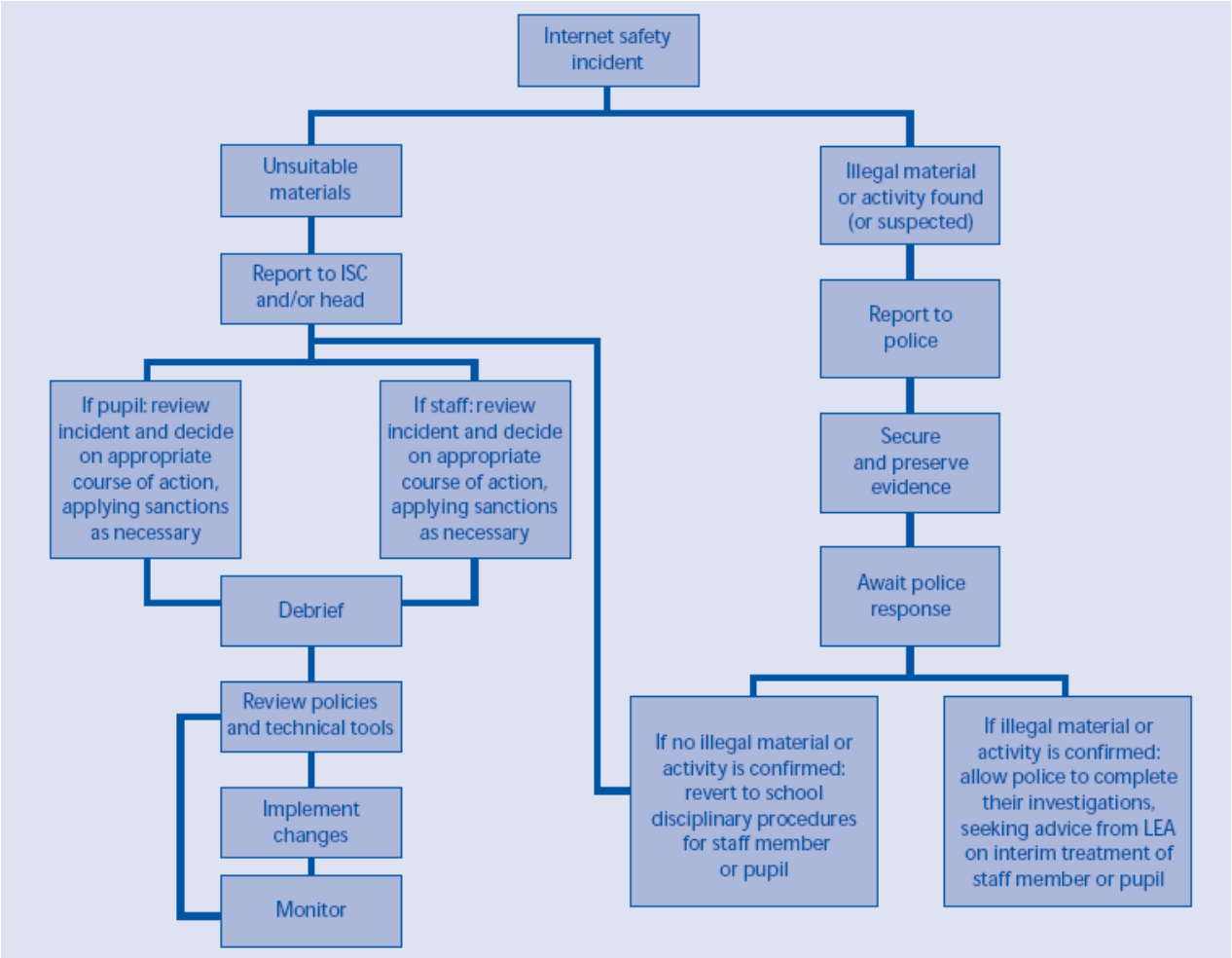
- When there has been a report of sexual violence, the designated safeguarding lead (or a deputy) should make an immediate risk and needs assessment. Where there has been a report of sexual harassment, the need for a risk assessment should be considered on a case-by-case basis.

- The school will carefully consider any report of sexual violence and/or sexual harassment both online and offline, including those that have happened outside of school.

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	
	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 / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

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

The following flow diagram shows the procedure for responding to incidents of misuse:



From E-safety Developing whole-school policies to support effective practice, Becta

14 Sanctions

- If a pupil misuses e-mail or the Internet, they must be reminded that this is irresponsible and contrary to their agreement with the Online Presence and Internet-enabled Devices Police. They must agree to responsibly use the Internet and a further copy of the Online Presence and Internet-enabled Devices Policy will be sent home for the child and parent to sign. A record of misuse will be logged by the Internet security co-ordinator. The child will not be allowed to resume the use of the Internet until the AUP has been resigned by the parent and child. Minor transgressions can be dealt with by the teacher as part of normal school discipline policy.

- In serious circumstances the privileges of Internet use will be withdrawn for a fixed period of time.

15. Monitoring

- The Internet Safety Co-ordinator will monitor any logged incidents and assess their importance.
- Pupils will be informed their Internet use can be monitored. Monitoring checks will be made if any inappropriate use is suspected.

- The Internet Safety Co-ordinator will report on incidents and the effectiveness of the e-safety policy to the governing body on an annual basis.

Review

Due to the nature of the Internet and developing technologies this policy will be reviewed on an annual basis.

References and resources

Keeping Children Safe in Education (updated September 2024)
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
Working together to Safeguard Children 2023
https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101457/KCSIE_2022_Part_One.pdf

https://www.gov.uk/government/collections/primary-school-teachers-useful-information

Sexual harassment and Sexual Violence (updated September 2021)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101667/WITHDRAWN_Sexual_violence_and_sexual_harassment_between_children_in_schools_and_colleges.pdf

https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

SWGfL Online Safety School Policy Template
https://swgfl.org.uk/online-safety-policy-templates-for-schools/#download-documents

'E-safety - Developing whole-school policies to support effective practice', Becta

Signposts to Safety – Teaching e-safety at KS1 and 2', Becta

Kent National Grid for Learning – Schools Internet Policy 5th Edition

www.becta.org.uk

www.pin-parents.com

www.nchafc.org.uk/Internet/index.html

www.vodaphone.com/content/parents.html

www.childnet.com/parents-and-carers

www.saferinternet.org.uk/advice-and-resources/parents-and-carers

www.thinkuknow.co.uk/parents

Online Presence and Internet-enabled Devices Policy

2022/23

The Admission Policy is based on best practice advice from Lancashire County Council.

The implementation of this policy will be monitored by Mrs Holt in consultation with the Leadership Team and a nominated Governor.

This policy will be reviewed as appropriate by The Faith & Community Committee

Intended Policy Review Date – May 2025

Approved by _____ (Headteacher)

Date: _____

Approved by _____ (Governor)

Date: _____