Emmaus Catholic and Church of England Voluntary Aided Academy

Online Safety policy and other supporting policies and documents.

2022

Policy Introduction

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include-

- The Internet
- E-mail
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites/apps (Popular Facebook, Instagram, Kik)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms
- Gaming Sites (Popular, http://www.miniclip.com/games/en/, http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www-kazzaa.com/, http://wwwlivewire.com/)
- Mobile phones with camera and video functionality
- Games consoles that are 'internet ready', enabled for pupils to play others across the world.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

As a school, we must demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. This online safeguarding policy explains how we intend to do this, while also addressing wider educational issues in order to help young people, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

Scope of the Policy

This policy applies to all stakeholders associated with our School and their responsibilities for complying with it. In particular-

- This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other online safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others.
- The school identifies within this policy and in the associated behaviour and anti-bullying policy, how incidents will be managed and will, where known, inform parents / carers of incidents of inappropriate online safeguarding behaviour that take place out of school.
- The policy should be read in-conjunction with other school policies, including the curriculum policy, safeguarding policy, behaviour and anti-bullying policy and information management policies.

Development / Monitoring / Review of this Policy

This policy has been developed by a working group (Safeguarding and online safety Team) made up of:

- School Online Safety Coordinator
- Computing Subject Lead
- Headteacher / Senior Leadership Team
- Governors

Consultation with the whole school community has taken place through the following:

- Staff meetings
- INSET Day
- School Council
- Governors meeting
- School website
- Lunch Time Supervisor meeting
-

Schedule for Development / Monitoring / Review

Title	**Online safety Policy**
Version	1.1
Date	January 2021
Author	*Online Safety Co-ordinator/Team*
This online safety policy was approved by the Governing Body on*:*	25.02.21
Monitoring will take place at regular intervals (at least annually):	Annually and sooner if any online safety incidents occur.
The Governing Body will receive a report on the implementation of the policy including anonymous details of any online safety incidents at regular intervals:	Headteacher's Report to Governors Termly
The 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 2022**
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Sheffield Safeguarding Team* *Police Commissioner's Office*

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS)
- Internal monitoring data for network activity e.g. Smoothwall
- Surveys / questionnaires of pupils/ parents / carers /staff

All staff and members of the School community must be informed of any relevant amendments to the policy.

Communication of the Policy

All amendments will be discussed and reviewed by the Online Safeguarding coordinator and the school's senior leadership team and then circulated and discussed with teaching staff and other members of the school community when it is considered appropriate.

- Emmaus Catholic and Church of England Primary School's senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school Online Safeguarding policy and the use of any new technology within school.
- The Online Safeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- Online Safety will be included in the PSHE, Citizenship and Computing curricula covering and detailing amendments to the Online Safeguarding policy.
- Annual Online Safety briefings will be established across the school.
- Pertinent points from the school Online Safeguarding policy will be reinforced across the curriculum, including the online safeguarding curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the Online Safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed Online Safeguarding messages across the curriculum whenever the internet or related technologies are used.
- The Online Safeguarding messages will be shared with pupils during assemblies, as well as in class.
- Safeguarding posters will be displayed around the school and key messages will be communicated to parents via the school website or other forms of school communication (email, text, letter, face to face).

Roles and Responsibilities

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

We believe that online safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team:

- The Headteacher has overall responsibility for online safety all members of the school community, though the day to day responsibility for online safety will be delegated to the online safety Co-ordinator.
- The headteacher and senior leadership team are responsible for ensuring that the online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues when necessary.
- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the online safety Coordinator.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious online safety incident.
- The headteacher and senior leadership team should receive update reports from the incident management team.

Responsibilities of the online safety Coordinator (Joanna Kenton)

- To ensure that the school Online Safeguarding policy is current and pertinent.
- To ensure that the school Online Safeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.
- To promote an awareness and commitment to Online Safeguarding throughout the school.
- To be the first point of contact in school on all Online Safeguarding matters.
- To take day-to-day responsibility for Online Safeguarding within school and to have a leading role in establishing and reviewing the school Online Safeguarding policies and procedures.
- To have regular contact with other Online Safeguarding committees, e.g. Safeguarding Children Board
- To communicate regularly with school technical staff (ACS).
- To communicate regularly with the designated Safeguarding governor
- To provide updates to Governors with annual training.
- To communicate regularly with the senior leadership team.
- To develop an understanding of current Online Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of knowledge in Online Safeguarding issues.
- To ensure that Online Safeguarding education is embedded across the curriculum.
- To ensure that Online Safeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online Safeguarding issues via Smoothwall and report back to the Headteacher if needed.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safeguarding incident.
- To ensure that an Online Safeguarding incident log is kept up to date (recorded in CPOMS

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote the school's online safety policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the online safety coordinator.
- To develop and maintain an awareness of current online safety issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed online safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff (ACS group)

- To read, understand, contribute to and help promote the school's online safety policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any online safety related issues that come to your attention to the online safety coordinator.
- To develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, work placement students and volunteers

Communication between adults and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff and volunteers should:

- Only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- Not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).

- Staff will not send or accept a friend request from the child/young person on social networks.
- Staff will ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the school into disrepute.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with children so as to avoid any possible misinterpretation.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Designated Safeguarding lead

- To understand the issues surrounding the sharing of personal or sensitive information in line with the General Data Protection Regulation (GDPR) 2018.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of Pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of online safety policies and practices and to adhere to any policies and practices the school creates.
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies on the taking and use of mobile phones.
- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss online safety issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting online safety.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.

- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss online safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology.
- To consult with the school if they have any concerns about their children's use of technology.

Responsibilities of the Governing Body

- To read, understand, contribute to and help promote the school's online safety policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the online safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety activities.
- To ensure appropriate funding and resources are available for the school to implement its online safety strategy.

The role of the Online Safety Governor includes:

- Regular meetings with the Online safety Co-ordinator.
- Regular monitoring of Online Safety incident logs.
- Reporting to Governors meeting.

Education

Pupils

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

Online safety education will be provided in the following ways:

- We will provide a series of specific online safety -related lessons in every year group/specific year groups as part of the ICT curriculum / PSHE curriculum / other lessons.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

All Staff (including Governors)

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.
- An audit of the online safety training needs of all staff will be carried out annually.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.
- 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 as required to individuals as required.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through

- parents' evenings
- newsletters
- letters
- website
- information about national / local online safety campaigns / literature

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems should be based upon a 'least privilege' approach.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive. **From Key Stage 1, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy**. They will ensure they log out after each session.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Smooth Wall.
- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the online safety Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the online safety Coordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP Child Exploitation and Online Protection Command or the IWF Internet Watch Foundation.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the IWF list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

- A secure and robust username and password convention exists for all system access. (Email, network access, school management information system).
- Pupils at Key Stage 1 and above will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users 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.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.

- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + =, < >: "'): the more randomly they are placed, the more secure they are.

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Data Protection

Personal Data

The school may have access to a wide range of personal information and data, held in digital format or on paper records. Being transparent and providing accessible information to individuals about how we will use personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation 2018 (GDPR). Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children / young people, members of staff / volunteers / students and mothers and fathers / carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by mothers and fathers / carers or by other agencies working with families

Settings that work with children and young people are likely to be under greater scrutiny in their care and use of personal data, following high profile incidents. The GDPR 2018 allows for a maximum fine of €20 million (APPROX. £18 million) for breaches of information security for both public and private sector organisations. All schools must understand the implications of not securing the information assets they hold and must to appoint a Data Protection Officer (DPO). This role may well be combined with the school's Data Protection Officer and, where appropriate, Information Asset Owners (IAO)

Our DPO officer is John Walker – please contact the school office for further information.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is a member of the senior leadership team who is familiar with information risks and the organisation's response. They have the following responsibilities

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management

The Office of Public Sector Information has produced a publication 'Managing Information Risk' to support SIROs in their role.

Information Asset Owner (IAO)

There is an IAO for each asset or group of assets within school. For example, the school's management information system should be identified as an asset and should have an IAO. The role of an IAO is to understand

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why

- How information is retained and disposed of

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

School will:

- 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 or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.

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

  - The data must be encrypted and/or 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.

- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email or post) will be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

If you are transmitting sensitive information or personal data e.g. by email or fax it must be transferred by a secure method so it is protected from unauthorised access.

Email

It is advisable not to use public email accounts for sending and receiving sensitive or personal data.

DO NOT include personal or sensitive information within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

Encryption makes a file non-readable to anyone who does not have the password to open it, therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices	X No mobiles						X	
Use of hand held devices e.g. PDAs, PSPs	x							x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails		x						x
Use of chat rooms / facilities in lessons				x				x
Use of instant messaging in lessons				x				x

Use of social networking sites in lessons				x				x
Use of blogs in lessons		x					x	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below (See Table 1 and 2) are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

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

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that our 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.

Table 1

Students / Pupils Actions / Sanctions

Incidents:	*Inform class teacher ordinator/ safeguarding team or assistant headteacher*	*Refer to Headteacher*	*Refer to police*	*Refer to technical support staff for action re filtering / security etc.*	*Inform parents / carers*	*Removal of network / internet access for a period of time*	*Warning / lost Golden Time/ White Form*	*Further sanction e.g. exclusion*
Deliberately accessing or trying to access material that could be considered illegal.	✓ ✓	✓			✓		✓	
Unauthorised use of non-educational sites during lessons	✓ ✓					✓	✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓ ✓	✓			✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓ ✓				✓		✓	
Unauthorised downloading or uploading of files	✓ ✓			✓	✓		✓	
Allowing others to access school network by sharing username and passwords	✓ ✓			✓		✓	✓	
Attempting to access or accessing the school network, using another student's / pupil's account	✓ ✓	✓		✓	✓	✓	✓	
Attempting to access or accessing the school network, using the account of a member of staff	✓ ✓	✓		✓	✓	✓	✓	✓
Corrupting or destroying the data of other users	✓ ✓	✓		✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓ ✓	✓	✓		✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓ ✓	✓	✓		✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓ ✓	✓			✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓ ✓	✓			✓		✓	
Deliberately accessing or trying to access offensive or pornographic material	✓ ✓	✓	✓		✓	✓	✓	✓

Table 1

Staff Actions / Sanctions

Incidents:	*Refer to Headteacher*	*Refer to Online safety Co-ordinator or safeguarding team member*	*Refer to Local Authority / HR*	*Refer to Police*	*Refer to Technical Support Staff for action re filtering etc*	*Warning*	*Suspension*	*Disciplinary action*
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓			✓		✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				✓		✓
Unauthorised downloading or uploading of files	✓	✓				✓		✓
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	✓	✓				✓		✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓	✓			✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓					✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓					✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓		✓				✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓	✓				✓	✓
Actions which could compromise the staff member's professional standing	✓	✓	✓			✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓			✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓		✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓	✓	✓

Emmaus Catholic and C of E Primary School

Year 3, 4, 5 and 6

Pupil ICT Acceptable Use Policy 2021

For my own safety:

- I understand that the school will watch my use of ICT, email and other digital communications. An adult will be supervising my use at all times.
- I will not share my username and password with anyone or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am on-line.
- I will not share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any upsetting or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that school ICT is for teaching and learning and I will not use it for personal or use unless I have permission to do so.
- I will not use the school ICT systems for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will respect other people's work and property and will not access, copy, remove or otherwise alter anyone else's files, without the owner's permission.
- I will be polite and responsible when I communicate with others.
- I will not take images of anyone without their permission.

I understand that the school has a responsibility to keep ICT secure and safe:

- I will only use my personal devices (mobile phones / USB devices / smart watches etc.) in school if I have permission. I understand that, if I do have my own devices in school, I will follow the rules and hand it in to my class teacher or to the school office.
- I will immediately report any damage or faults involving equipment, however it may have happened.
- I will not open any attachments to emails, unless I know and trust the sender of the email.
- Social Networking sites are not allowed to be used in school.

When using the internet for research for my school work, I understand that:

- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.

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

- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this is cyberbullying, sending/receiving inappropriate images and misuse of personal information.

- I understand that I must follow these rules. If I don't this could mean loss of access to the school network / internet, contact with parents/carers and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have understood and agree to the rules included in the Acceptable Use Agreement.

I understand the rules and I agree to follow these rules when:

- I use school ICT and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.

Name of Student / Pupil			
Group / Class			
Signed		Date	

Emmaus Catholic and C of E

Primary School

Year 1 and 2

Pupil ICT Acceptable Use Policy 2021

This is how we stay safe when we use computers:

I will ask an adult if I want to use the computer.

An adult will watch me using the ICT equipment.

I will only use activities that an adult has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

I will tell an adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):

Signed (parent): ……..

Think before you click

S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Legislation

Schools should be aware of the legislative framework under which this Online-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990 This Act makes it an offence to:
• Erase or amend data or programs without authority;
• Obtain unauthorised access to a computer;
• "Eavesdrop" on a computer;
• Make unauthorised use of computer time or facilities;
• Maliciously corrupt or erase data or programs;
• Deny access to authorised users.

General Data Protection Regulation (GDPR) 2018
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
• Fairly and lawfully processed.
• Processed for limited purposes.
• Adequate, relevant and not excessive.
• Accurate.
• Not kept longer than necessary.
• Processed in accordance with the data subject's rights.
• Secure.
• Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000 It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
• Establish the facts;
• Ascertain compliance with regulatory or self-regulatory practices or procedures;
• Demonstrate standards, which are or ought to be achieved by persons using the system;
• Investigate or detect unauthorised use of the communications system;
• Prevent or detect crime or in the interests of national security;
• Ensure the effective operation of the system.
• Monitoring but not recording is also permissible in order to:
• Ascertain whether the communication is business or personal;
• Protect or support help line staff.
• The school reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances

permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -
• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986 This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:
• The right to a fair trial
• The right to respect for private and family life, home and correspondence
• Freedom of thought, conscience and religion
• Freedom of expression
• Freedom of assembly
• Prohibition of discrimination
• The right to education
These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.