



# St Mary's Priory Catholic Infant and Junior Schools

Love one another

Always do our best

Take care of ourselves and the world around us

Online Safety Policy

Date Agreed: March 2026

Date for Review: March 2027

## **Contents**

Introduction

Background/Rationale

Schedule for development, monitoring and review

Scope of the Policy

Roles and Responsibilities

- Governors
- HT, and Senior Leaders
- Online -Safety Co-ordinator
- Technical Staff
- Teaching and Support Staff
- Designated Person for Child Protection
- Pupils
- Parents/carers
- Community Users Policy
- Online Safety Group

Statements

- Education – Pupils
- Education – Parents/carers
- Education – Wider Community
- Education and training – Staff
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Curriculum
- Use of digital and video images
- Mobile Technologies
- Anti - Bullying
- Social Media
- Data Protection
- Reporting online safety incidents and concerns
- Unsuitable / inappropriate activities
- Responding to incidents of misuse

## Introduction

National guidance suggests that it is essential for schools to take a leading role in Online -Safety. Beeta in its "Safeguarding Children in a Digital World" suggested:

*"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, it is recommended that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, furthermore schools should take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

*"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. At St. Mary's Priory Catholic Infant & Junior Schools we have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks."

At St. Mary's Priory Catholic Infant & Junior Schools, our aim is to ensure that our children are safe and are protected from potential harm, both within and outside school. We believe that safe internet access is an entitlement for all learners.

The school recognises that Artificial Intelligence (AI), including generative AI systems, forms part of the modern digital landscape. AI technologies present both educational opportunities and safeguarding risks. The school has adopted a separate Safe Use of AI Policy which governs the secure, lawful and appropriate use of AI tools, including the approved use of Microsoft Copilot by staff. This Online Safety Policy should be read in conjunction with the Safe Use of AI Policy.

Due to the ever-changing nature of Information and Communication Technologies, it is best practice that the school reviews the Online-Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online -safety or incidents that have taken place.

## Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge (sexting, sextortion)
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online-safety policy is used in conjunction with other school policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Schedule for Development/Monitoring/Review

The implementation of this Online-safety policy will be monitored by the:	E-Safety Coordinator / Senior Leadership Team/ Online safety Governor
---	---

Monitoring will take place at regular intervals:	At least once a year
--	----------------------

The Governing Body will receive a report on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at regular intervals:	At least once a year as part of HT report
--	---

The Online-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.	Spring Term following Safer Internet Day
--	--

The implementation and impact of AI technologies within the school will be reviewed annually alongside the Safe Use of AI Policy.

Should serious online-safety incidents take place, the following external persons / agencies should be informed:	Online safety Governor, Safeguarding Governor, SIA, LA Safeguarding Officer
--	---

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Pupil Voice
- Feedback from parents
- Feedback from staff

### Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

This policy also applies to the use of Artificial Intelligence (AI) systems, including generative AI tools, whether accessed through school devices, school networks, or used in connection with school-related activities.

The Education and Inspections Act 2006 empowers Senior Leaders, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

### Roles and Responsibilities

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

#### Governors:

Governors are responsible for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online-Safety. The role of the Online-Safety Governor will include regular updates from the Online-Safety Co-ordinator, The safeguarding governor will monitor online-safety incident logs. reporting to FGB.

Governors will also monitor the implementation of the Safe Use of AI Policy and receive updates regarding the use of approved AI systems within the school, including compliance with data protection and safeguarding requirements.

#### HT and Senior Leaders:

- The HT is responsible for ensuring the safety (including online-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Online-Safety Co-ordinator
- The HT / Senior Leaders are responsible for ensuring that the Online-Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their online-safety roles and to train other colleagues, as relevant
- The HT will receive regular monitoring reports from the Online-Safety Co-ordinator.
- The HT will ensure that only approved AI platforms, as outlined in the Safe Use of AI Policy, are used for school-related purposes and that staff receive appropriate training regarding the safe and responsible use of AI tools.
- The Updates the safeguarding governor with regard to any issues

- The HT and the DHT should be aware of the procedures to be followed in the event of a serious Online -safety allegation being made against a member of staff. (see COLFS flow chart on dealing with e-safety incidents included in a later section – “Responding to incidents of misuse” and relevant disciplinary procedures)

#### Online - Safety Co-Ordinator:

- takes day to day responsibility for online-safety issues and has a leading role in establishing and reviewing the school Online -safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online-safety incident taking place. Any investigation/action/sanctions will be the responsibility of the HT or DHT
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of online-safety incidents and creates a log of incidents to inform future online-safety developments.
- review incident logs and report regularly to Senior Leadership Team
- The Online-Safety Co-ordinator will work alongside the Digital Lead and Designated Safeguarding Lead to monitor and respond to any online safety concerns arising from the use of AI tools.

#### Data Protection Officer (DPO)

##### Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ and ‘Data protection: a toolkit for schools’ (April 2018), especially this quote from the latter document:
- GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place [...] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding
- The same document states that the retention schedule for safeguarding records may be required to be set as ‘Very long-term need (until pupil is aged 25 or older)’
- Work with the DSL, SLT and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

#### Technical staff:

The ICT Technician is responsible for ensuring:

- that the school’s ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online-safety technical requirements outlined in any relevant Local Authority Online-Safety Policy and guidance(LGFL)
- Technical staff will ensure that unapproved AI tools are restricted via filtering systems where appropriate and that the approved AI platform operates within secure access and monitoring arrangements.
- that users may only access the school’s networks through a properly enforced password

protection policy, in which passwords are regularly changed

- that he/she keeps up to date with online-safety technical information in order to effectively carry out their online-safety role and to inform and update others as relevant

### Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school online-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the online-Safety co-ordinator/SLT
- digital communications should be on a professional level *and only carried out using official school systems*
- online-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extracurricular and extended school activities
- they are aware of online-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### Designated person for child protection:

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

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

### Online Safety Group

The Online Safety Group provides a consultative group that has a wide representation from St. Mary's Priory Catholic Infant & Junior Schools with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

- the production / review / monitoring of the school Online Safety Policy

**Online Safety Lead, DSL / SLT & Governors.**

- the production / review / monitoring of the school filtering policy and requests for filtering changes.

**Maintained by LGFL and reviewed by the Online Safety Lead, ICT Consultant, DSL & Senior Business & Operations Manager**

- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision

**Online Safety Lead & SLT**

**Maintained by LGFL and reviewed by the Online Safety Lead, ICT Consultant, DSL & Senior Business & Operations Manager**

**Online Safety Lead**

Members of the Online Safety Group will assist the Online Safety Co-ordinator/ Lead with:

Pupils:

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

Parents/carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. 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. We will attempt to take every opportunity to help parents understand these issues e.g. through parents' evenings, newsletters, letters, signposting literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy

Community Users:

Any Community Users who access school ICT systems as part of the extended school provision will be expected to sign a Staff/Visitor/Volunteer AUP before being provided with access to school systems.

**Policy Statements**

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. We aim to support our children in recognising and avoiding online-safety risks and build their resilience.

Online-Safety education will be provided in the following ways:

- Online-safety is delivered as part of the Computing curriculum and are regularly revisited
- The national annual safer internet day is used as a focus to impart key online-safety messages
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be displayed on all computer screens before logging in
- Staff should act as good role models in their use of ICT and the internet and any mobile devices

### Education–parents/carers

Many parents and carers have only a limited understanding of online-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

St. Mary's Priory Catholic Infant & Junior Schools are committed to supporting parents and carers. At St. Mary's Priory Catholic Infant & Junior Schools we believe that schools, parents and carers should work together to take an active role in teaching children about online dangers. Learning to act safely when using the internet is an incredibly important part of safeguarding our children. There is a dedicated Online Safety page on the St. Mary's Priory Catholic Infant & Junior Schools website which sign posts parents to key websites and resources that they can use at home. Many of these resources are linked to those used in school.

### Education – The Wider Community

St. Mary's Priory Catholic Infant & Junior Schools may provide opportunities for local community groups to gain from St. Mary's Priory Catholic Infant & Junior Schools's online safety knowledge and experience. This may be offered through the following:

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

### Education and Training–Staff

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.
- All new staff should receive online-safety training as part of their induction programme and fully understand the school online-safety policy and Acceptable Use Policies
- The Online-Safety Co-ordinator will receive regular updates of current practice
- This Online-Safety policy and its updates will be presented to and discussed by staff in staff meetings.

- The Online-Safety Co-ordinator will provide advice/guidance/training as required to individuals

### Training-Governors

Governors should take part in online-safety training/awareness sessions, with particular importance for those who are members of any group involved in ICT/e-safety/health and safety/ child protection.

### Technical-infrastructure/equipment, filtering and monitoring

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

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by the ICT technician who will keep an up-to-date record of users and their usernames. Users will be required to change their password annually.
- The administrator passwords for the school ICT system, used by the Network Manager must also be available to the HT and kept in a secure
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports a managed filtering service provided by LGFL
- The school will ensure that filtering and monitoring systems consider the use of AI technologies. Monitoring arrangements will include oversight of AI-related activity to ensure compliance with safeguarding, data protection and the Safe Use of AI Policy.
- Any filtering issues should be reported immediately to the Online-safety co-ordinator.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head Teacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online-Safety Co-Ordinator
- Agreed procedures are in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system.
- Only the ICT technician has permissions to install programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### Curriculum

Pupils will have regular discrete online-safety lessons that follow the Education for a Connected World framework which supports children in staying safe and making a positive contribution online, as well as equipping teachers with strategies to understand and deal with online risks.

The Educated for a Connected World framework *‘describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, it’s influence on behaviour and*

*development, and what skills they need to be able to navigate it'* quote taken from **UK Council For Internet Safety (February 2018)**.

Online-safety should be a focus in all areas of the curriculum and staff should reinforce online-safety messages in the use of ICT across the curriculum.

Pupils will be taught about Artificial Intelligence and generative AI technologies, including understanding their limitations, potential bias, reliability issues and the importance of critical evaluation. Pupils will be supported to understand how AI-generated content should be referenced appropriately and that AI tools cannot replace independent thinking and learning.

- in lessons where internet use is pre-planned, it is best practice that / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Requests should be made to the Head Teacher
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- This includes developing awareness that AI tools may generate inaccurate, misleading or biased content and that not all online information is reliable. Pupils will be taught how to question and verify AI-generated information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

### Use of digital and video images

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 be taken on school equipment. Personal equipment of staff can be used for such purposes but must be uploaded and deleted from personal devices, once uploaded.
- 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 pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names should 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.

### Mobile Technologies

Mobile technology devices may be school owned or personally owned and these include: smartphones, tablet, or other technology that usually has the capability of utilising the school's wireless network.

All staff and pupils should understand that the primary purpose of these mobile / personal devices in a school context is educational. The use of our mobile devices is consistent with the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- **The school Staff Code of Conduct and Acceptable Use Agreements give consideration to the use of mobile technologies**
- **The school allows:**

	School Devices		Authorise d device	Personal Devices		
	School owned for single user	School owned for multiple users		Studen t owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	No	Yes	No	No	No
Internet only	No	Yes	Yes	No	Yes	Yes

### Cyber Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy is followed for online bullying, which may also be referred to as cyberbullying (See Anti Bullying Policy and Behaviour Policy)

Regular sessions are delivered to both pupils and staff, to ensure reporting routes and responsibilities are clear and understood.

### Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

### Social Media

Social networking sites have potential to enhance the learning and achievement of pupils and enable parents to access information about the School and provide feedback efficiently and easily. In addition, the School recognises that many staff and parents will have personal social networking accounts, which they might use to discuss/share views about school issues with friends and acquaintances. See Social Media Policy as a guide to what staff and parents should consider prior to posting any information on social networking sites about the School, its staff, its pupils.

### Data Protection

Personal data will be recorded, processed, transferred and made available according the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016.

- 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.

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.
- Staff must not enter personal, sensitive, safeguarding or pupil-identifiable information into generative AI tools unless the platform has been formally approved by the school and reviewed by the Data Protection Officer.
- Only the approved version of Microsoft Copilot, as outlined in the Safe Use of AI Policy, may be used for school-related activities. Public or personal AI accounts must not be used for professional purposes.
- All AI-generated content remains the professional responsibility of the staff member using it and must be reviewed for accuracy, bias and appropriateness prior to use.
- Transfer data using encryption and secure password protected devices

### **Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. If staff have any concerns over the security of their device, they must seek advice in the first instance from the Computing /E safety Leader.

Work devices must be used solely for work activities.

### **GDPR**

There are references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ and ‘Data protection: a toolkit for schools’ (April 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

“GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place [...] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding.”

All pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy.

Rigorous controls on the LGfL TRUSTnet network, USO sign-on for technical services, firewalls and filtering all support data protection. The HT, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

## **Reporting online-safety concerns and incidents**

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of caution by talking to the online-safety lead and the designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made immediately.

Any concern/allegation about staff misuse is always referred directly to the HT, unless the concern is about the HT in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

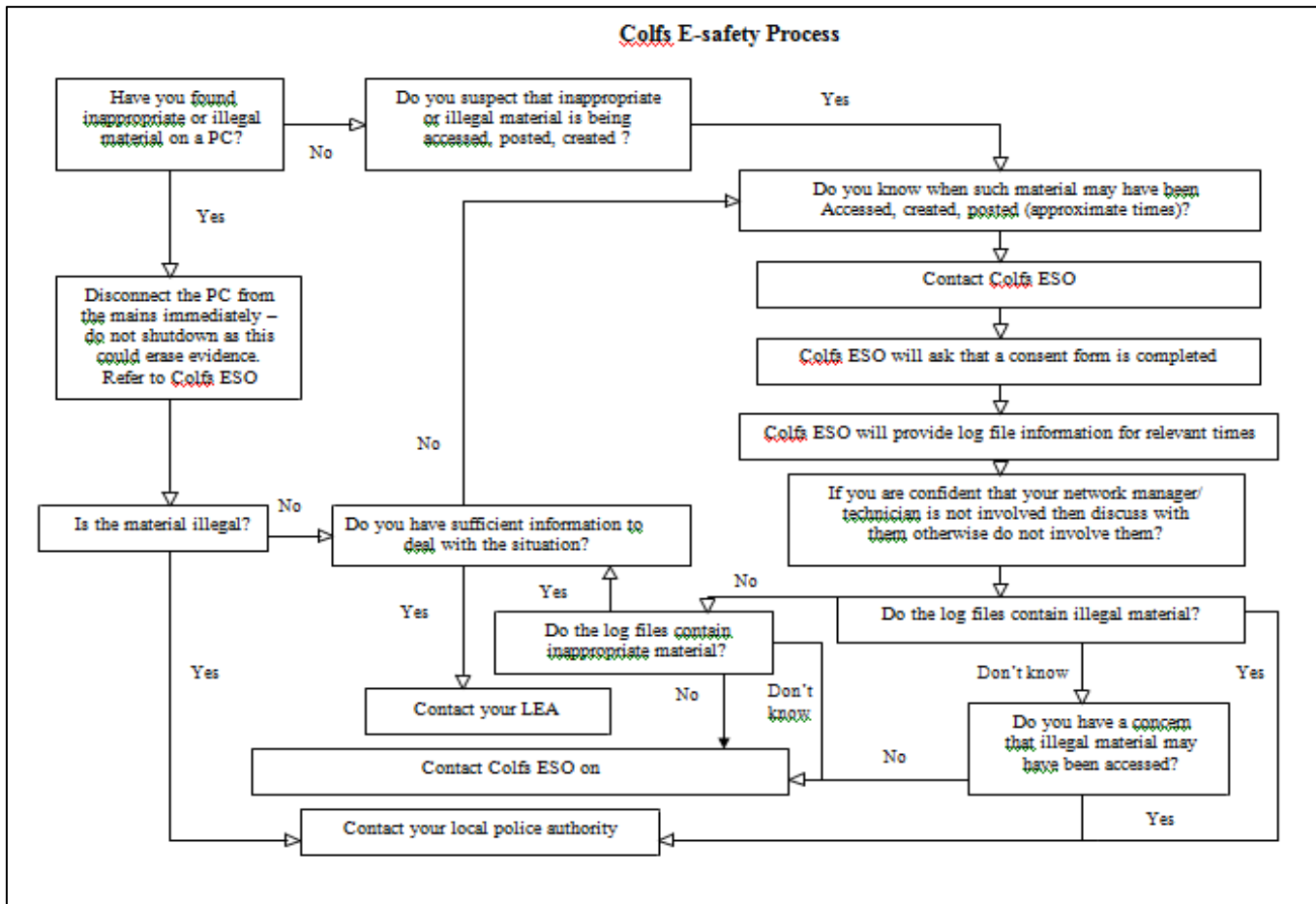
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

## **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. Misuse of AI tools, including submitting AI-generated content as independent work, using unapproved AI systems, or inputting personal data into unauthorised platforms, will be managed in accordance with the Safe Use of AI Policy and relevant disciplinary procedures.

If any apparent or actual misuse appears to involve illegal activity (i.e. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material, other criminal conduct, activity or materials), the flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

### Colfs E-safety Process



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/ disciplinary procedures (See Behaviour Policy, Anti Bullying Policy)

## Pupil Acceptable Use Policy Agreement – KS1 / Foundation

### School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### KS1 / Foundation

These rules will be shared with the children by the staff who work in Key Stage 1. Children will be reminded of them when required. Rules will be on display by the computers so all staff/volunteers are aware of what the children are allowed to do and what rules to reinforce.

To stay **SAFE** online and on my devices, I:

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** in front of a camera or share pictures of myself
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone

### Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment
- 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,

Name of Pupil

Class

Signed

Date

## Pupil Acceptable Use Policy Agreement – KS2

### School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### KS2

These rules will be shared with the children by the staff who work in Key Stage 2. Children will be reminded of them when required. Rules will be on display by the computers so all staff/volunteers are aware of what the children are allowed to do and what rules to reinforce.

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.
23. I understand that AI tools can make mistakes or give biased information. If I use AI tools, I will follow my teacher's guidance and make sure my work shows my own understanding.

Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment
- 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,

Name of Pupil

Class

Signed

Date

## **Acceptable Use Policy Agreement Staff, Governors & Volunteers**

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff, Governors and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff, Governors and volunteers are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, Governors and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement staff, Governors & Volunteers

I understand that I must use school ICT systems in a responsible way, to ensure that there

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of St. Mary's Priory Catholic Infant & Junior Schools ICT systems (e.g. laptops, email) out of St. Mary's Priory Catholic Infant & Junior Schools
- I understand that the schools ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems:
- I understand that only the school-approved version of Microsoft Copilot may be used for professional purposes. I will not use public or personal AI accounts for school work.
- I will not input personal, sensitive or safeguarding data into AI systems.
- I understand that any AI-generated content I use remains my professional responsibility.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal

equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school's in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school emails. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- When I use my personal hand held / external devices (mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)
- I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT

equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police
- I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

--

Signed

--

Date

--

## Parental Acknowledgement

Name of Pupil

Class

As the parent / carer of the above, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will continue to receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date