# ONLINE SAFETY POLICY

**Note: Policy to be read in conjunction with the Plymouth CAST Code of Conduct for Staff Policy**

Adopted: November 2020 Lorna Wilby
Review date: November 2021

## Contents


**Section 1** 1.1 Background/Rationale
1.2 Development, monitoring and review of the Policy
1.3 Schedule for development, monitoring and review
1.4 Scope of the Policy

**Section 2** **Roles and Responsibilities**

2.1 Governors
2.2 Principal and Senior Leaders
2.3 Designated Online Safety Coordinator
2.4 Network Manager/Technical Staff
2.5 Teaching and Support Staff
2.6 Designated Person for Child Protection
2.7 Online Safety Committee
2.8 Children
2.9 Parents/Carers

**Section 3** **Policy Statements**

3.1 Education – Children
3.2 Education – Parents/Carers
3.3 Education and training – Staff
3.4 Training – Governors
3.5 Technical – infrastructure/equipment, filtering/monitoring
3.6 Curriculum
3.7 Use of Google Apps For Education
3.8 Use of digital and video images
3.9 Data protection and cloud based storage
3.10 Child Sexual Exploitation
3.11 Communication Technologies
3.12 Unsuitable/inappropriate activities
3.13 Responding to incidents of misuse

Appendix 1 - Acceptable Use Agreement: Pupils
Appendix 2 - Acceptable Use Agreement: Parent/Carer
Appendix 3 - Acceptable Use Agreement: Staff, Governors and Visitors



Adopted: November 2020 Lorna Wilby
Review date: November 2021

**SAFEGUARDING**
The Online Safety Policy at Our Lady's Catholic Primary School forms part of our Safeguarding Policy Portfolio and demonstrates our commitment to safeguarding the wellbeing of all our pupils.

## Section 1

### 1.1 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 children 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 requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our school Online Safety policy aims to help ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

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
- Inappropriate communication/contact with others, including strangers
- Online 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
- Sexting – sending sexually explicit photographs or messages.

Many of these risks reflect situations in the off-line world and as such it is essential that this Online Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection 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.

Adopted: November 2020 Lorna Wilby
Review date: November 2021

The school will demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

## 1.2 Development, Monitoring, Review of this Policy

This Online Safety policy has been developed by:

- Rob Meech - Principal
- Lorna Wilby - Online Safety Co-ordinator

Consultation with the whole school community will take place through the following:

- Staff meetings
- School Council
- Full Local Governing Board Meetings
- Computing Co-ordinator
- Parents consultation
- School website/newsletters

## 1.3 Schedule for Development, Monitoring, Review

| | |
|---|---|
| This Online Safety policy was approved by the Local Governing Body on*:* | Date: 25th November 2020 |
| The implementation of this Online Safety policy will be monitored by the: | Lead Governor for Safeguarding: – Simon Cohen<br>Local Governing Board |
| Monitoring of this policy will take place at regular intervals: | Termly |
| The Full Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents). | Annually |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be: | Annually |

| | |
|---|---|
| Should serious Online Safety incidents take place, the following external persons/ agencies should be informed: | South West Grid for Learning<br>Police Commissioner's Office |

The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS and reported to Governors in the Principal's Report
- Surveys/questionnaires of Children
- Parent/Carer Surveys
- Staff feedback

Adopted: November 2020 Lorna Wilby
Review date: November 2021

## 1.4 Scope of the Policy

This policy applies to all members of the school community (including staff, children, volunteers, visitors, community users) who have access to and are users of school computing systems, both in and out of school. The policy outlines acceptable use and the Acceptable Use Agreements are an appendix.

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of children 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 Online bullying, or other Online 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 online behaviour that take place out of school.

# Section 2: Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

## 2.1 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Local Governing Board, who may delegate this to appropriate governors/staff, receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor (Lead Governor for Safeguarding). The role of the Online Safety Governor will include:

- Governor visits
- Meetings as necessary with the designated Online Safety Co-ordinator
- Monitoring of Online Safety incident logs (through the use of CPOM)
- Reporting to the Full Local Governing Board

## 2.2 Principal and Senior Leaders

- The Principal is responsible for ensuring the safety of members of the school community. The day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.
- The Principal is responsible for ensuring that the Online Safety Coordinator 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 Principal is responsible for carrying out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Principal will receive monitoring reports from the Online Safety Co-ordinator.
- The Principal and another member of the Senior Leadership Team/Senior Management Team are aware of the procedures to be followed in the event of a serious Online Safety allegation

being made against a member of staff. Refer to Allegations against Staff in the Safeguarding Policy.

## 2.3 Designated 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.
- Provides training and advice for staff which may be delegated to other suitably qualified members of staff.
- Liaises with school Computing Co-ordinator and technical provider.
- Receives reports of Online Safety incidents and with the Principal creates a log of incidents to inform future Online Safety developments.
- Attends relevant meeting/committee of Governors when appropriate.
- Reports regularly to Head teacher.

## 2.4 Network Manager

The Network Manager (Computeam) 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 appropriate Online Safety standards and policy.
- Keeping 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.
- That the network is monitored on an ongoing basis so that any misuse/attempted misuse can be identified and reported to the Online Safety Co-ordinator.
- That monitoring software is appropriate and updated as necessary.

## 2.5 Staff

Staff are responsible for ensuring that:

- They have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Agreement (see appendix 3).
- They report any suspected misuse or problem to the Online Safety Co-ordinator or other designated person.
- Digital communications with children are only carried out within the context of their job role and at a professional level.
- Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- Children understand and follow the school Online Safety and Acceptable Use Agreement (see appendix 1).
- Children apply appropriate research skills that avoid plagiarism and uphold copyright regulations.
- They monitor Online Safety 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 and implement this policy with regard to these devices.
- In lessons where computing is used children should be, where practicable, instructed to use sites that have been pre checked as suitable for their use.
- That processes within the school are in place for dealing with any unsuitable material that is found in internet searches.

## 2.6 Designated Child Protection Officer

The designated Child Protection Officer is the Principal and is trained in Online Safety issues and is aware of the potential for serious child protection issues to arise from:

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

## 2.7 Children

- 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 technology including computers, mobile phones, digital cameras and hand held devices such as tablets. They should also know and understand school policies on the taking/use of images, sharing information and online bullying.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

## 2.8 Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take appropriate steps, where possible, to help parents understand these issues through parent communication and the school website. Parents and carers will be responsible for:

- Endorsing (by signature) the Acceptable Use Agreement (see appendix 2).

## Section 3: Policy Statements

### 3.1 Education – Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children 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 their parents/carers and school to recognise and avoid Online Safety risks and build their resilience. Online Safety education will be provided in the following ways:

- Planned Online Safety guidance will be part of Computing and reviewed annually – this will cover both technologies in school and outside school.
- Key Online Safety messages will be reinforced through a planned programme of activities.
- In lessons where computing plays a component part children will be taught to be aware of the materials/content they access online and be guided to validate the accuracy of information.
- Children will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of the internet and mobile devices both within and outside school.
- Children will be taught the need 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 reinforced in all classrooms.
- Staff should act as good role models in their use of the internet and mobile devices.

### 3.2 Education – parents/carers

The school will, where possible, work with parents and carers to ensure that the good Online Safety practices developed in school are practiced by children at home and outside of the school day.

### 3.3 Education and Training – Staff

It is the responsibility of all staff that they attend Online Safety training and understand their responsibilities, as outlined in this policy. Training will be mandatory as follows:

- All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the Online Safety policy and Acceptable Use Agreement (see appendix 3).
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at information/training sessions and by reviewing guidance documents released by SWGFL and DFE.
- This Online Safety policy and its updates will be presented from time to time in meetings that all staff must attend.
- The Online Safety Co-ordinator will provide advice/guidance/training as required to individuals as necessary.

### 3.4 Training – Governors

Governors will take part in Online Safety training/awareness sessions to be offered in a number of ways:

- Attendance at training events provided by external experts.
- Participation in school training/information sessions for staff or parents delivered at the school by Online Safety Co-ordinator or other professionals.

## 3.5 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 to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

- School systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined by SWGFL and the Acceptable Use Agreements (see appendix)
- School systems will be regularly updated to ensure up-to-date anti-virus definitions and Security Updates are installed.
- Essential software i.e. Acrobat Reader, Flash Player, Java, Web Browsers, Smart board etc. will be kept current
- There will be regular reviews and audits of the safety and security of school systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school systems
- The "master/administrator" passwords for the school system, used by the Network Manager will also be available to the Principal and kept in a secure place
- School Data should be securely managed when taken off the school site
- 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 the managed filtering service provided by the South West Grid for Learning
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal
- Any filtering issues should be reported immediately to the South West Grid for Learning
- Requests from staff for sites to be added or removed from the filtered list will be considered by the Principal.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data

## 3.6 Curriculum

- Online Safety should be a focus in all relevant areas of the curriculum and staff should take any opportunity to reinforce the Online Safety messages when technology is used in a cross-curricular context.
- Online Safety should be taught regularly with identified progression of knowledge, skills and understanding.
- Online Safety skills should be embedded through computing and cross-curricular application.

- In lessons where internet use is pre-planned, it is best practice that children 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 children are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites visited.
- Children should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Where appropriate children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

## 3.7 Use of Google Apps For Education (GAFE)

We are partnered with Google Apps for Education (GAFE) to provide productivity and collaboration tools to students in a safe, structured, and advertisement free manner.
GAFE is a suite of free online applications which are accessed through a web browser. Children from Reception to Year 6 are provided and educated in using a GAFE account. Our Lady's GAFE domain (@olcs) is set up so that students cannot share files and send/receive email to/from the public. File sharing and email correspondence can only occur between Our Lady's teachers and students. Email is not intended for communication between parents/guardians and their children, it is for educational purposes only.

## 3.8 Use of digital and video images - Photographic, Video

Staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about the risks of posting/sharing digital images and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate children 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.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's 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 children are published on the school website or social media.

## 3.9 Data Protection, GDPR and cloud based storage

Personal data will be recorded, processed, transferred and made available according to the requirements of the Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes

• Adequate, relevant and not excessive
• Accurate and up to date
• Kept no longer than is necessary
• Processed in accordance with the data subject's rights
• Secure
• Only transferred to others with adequate protection

School and children data may be stored and controlled in the cloud by a supplier. Our Lady's service providers include Google and CPOMS. These suppliers both comply with the DPA and GDPR and have completed self-certification checklists in relation to data protection competencies.

Staff must ensure that they:
- 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.
- Only transfer data outside of school 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 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

## 3.10 Child Sexual Exploitation

The internet is facilitating a major increase in children and young people being exposed to a wide range of inappropriate or illegal sexual and other kinds of material.

The sexual exploitation of children and young people under 18 involves exploitative situations, contexts and relationships where young people (or a third person/s) receive 'something' (e.g. food, accommodation, drugs, alcohol, affection, gifts, money) as a result of performing, and/or others performing on them, sexual activities. (The National Working Group for Sexually Exploited Children and Young People, 2008)

Online Sexual Exploitation includes:
- Befriending through online chat rooms/messaging services
- Online grooming techniques
- Asking children to take and share indecent images of themselves
- Leverage for further demands
- Arranging offline meeting for purpose of sexually abusing child
- Contact from perpetrators in other countries and abused online
- Speed of grooming can be very quick - leaving little 'thinking time'

Safeguarding policies ensure safeguarding staff are identified and known, regularly training and updates are provided, all staff are made aware of and understand CSE indicators and referral pathways, pupils are taught about online safety including peer pressure, bullying etc. and pupils know who to go to for help and support.

## 3.11 Communication Technologies

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

| | Staff & other adults | | | | Children | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies (outside of those available on the learning platform) | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | ☐ | | | | | | ☐ | |
| Use of mobile phones in lessons | | | | ☐ | | | | ☐ |
| Use of mobile phones in social time | | ☐ | | | | | | ☐ |
| Taking photos/film on mobile phones or other personal camera devices | | | | ☐ | | | | ☐ |
| Taking photos/film on school camera devices | ☐ | | | | | ☐ | | |
| Use of hand held school devices e.g. ipad. | ☐ | | | | | | ☐ | |
| Use of personal hand held devices | | ☐ | | | | | | ☐ |
| Use of personal email addresses in school, or on school network | | | | ☐ | | | | ☐ |
| Use of school email for personal emails | | | | ☐ | | | | ☐ |
| Use of chat rooms/facilities | | | | ☐ | | | | ☐ |
| Use of instant messaging | | | | ☐ | | | | ☐ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Use of social networking sites for educational purposes | | □ | | | | | | □ |
| Use of blogs for educational purposes | □ | | | | | | □ | |

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

- Where available the official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Class Teacher and Principal – 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 children or parents/carers must be professional in tone and content.
- Children are to be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

## 3.12 Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | **child sexual abuse images** | | | | | |
| | **promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation** | | | | | |
| | **adult material that potentially breaches the Obscene Publications Act in the UK** | | | | | |
| | **criminally racist material in UK** | | | | | |
| | **pornography** | | | | | |
| | **promotion of any kind of discrimination** | | | | | |
| | **promotion of racial or religious hatred** | | | | | |
| | **threatening behaviour, including promotion of physical violence or mental harm** | | | | | |
| | **any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **Using school systems to run a private business** | | | | □ | |
| **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGFL and/or the school** | | | | □ | |
| **Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions** | | | | □ | |
| **Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)** | | | | □ | |
| **Knowingly, creating or propagating computer viruses or other harmful files** | | | | □ | |
| **Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet** | | | | □ | |
| **Online gaming (educational) as defined by the Class Teacher** | | □ | | | |
| **Online gaming (non educational)** | | | | □ | |
| **Online gambling** | | | | □ | |
| **Online shopping/commerce (excluding the Office)** | | | | □ | |
| **File sharing (educational)** | | □ | | | |
| **Use of social networking sites (educational)** | | □ | | | |
| **Use of video broadcasting e.g. YouTube (educational)** | | □ | | | |

## 3.13 Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users, 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 are the responses that will be made to any apparent or actual incidents of misuse:

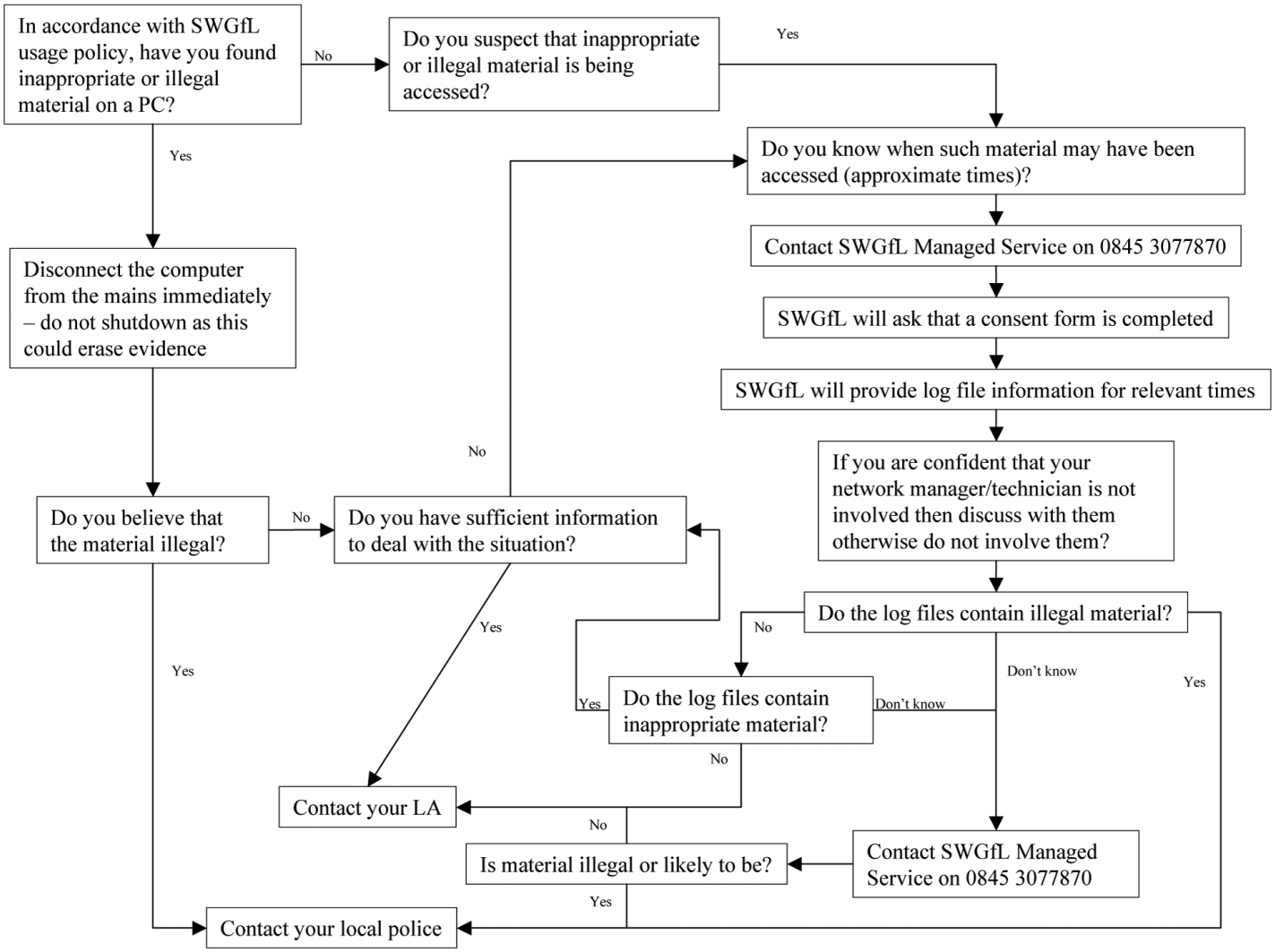
If any apparent or actual misuse appears to involve illegal activity i.e.

- 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 (to follow) – will 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.

Adopted: November 2020 Lorna Wilby
Review date: November 2021

**Our Lady's Catholic Primary School – Online Safety Reporting Concerns**




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 recommended that more than one member of staff is involved in 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 recorded on CPOMS and dealt with through normal behaviour/disciplinary procedures as follows:

Adopted: November 2020 Lorna Wilby
Review date: November 2021

## Children

| Incidents: | Refer to class teacher | Refer to Principal | Refer to Police | Refer to Network Manager for filtering/security etc. | Inform parents | Removal of network/ internet | Warning | Further sanction e.g. detention/exclusion |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).** | | ▯ | | | ▯ | ▯ | | ▯ |
| 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 the account of a member of staff | ▯ | ▯ | | | ▯ | ▯ | ▯ | |
| Corrupting or destroying the data of other users | ▯ | ▯ | | | ▯ | | ▯ | ▯ |
| Sending an email, text, instant message or equivalent 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 | ▯ | ▯ | | | ▯ | | | ▯ |
| 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 | ☐ | ☐ | ☐ | | ☐ | | | ☐ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act or GDPR | ☐ | ☐ | ☐ | | ☐ | | ☐ | |

## Staff

| Incidents: | Refer to Principal | Refer to HR | Refer to Police | Refer to Network Manager 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, instant message or equivalent 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 | ☒ | ☒ | ☒ | ☒ | | ☒ | ☒ |
| Breaching copyright or licensing regulations | ☒ | ☒ | | | ☒ | ☒ | ☒ |
| Continued infringements of the above, following previous warnings or sanctions | ☒ | ☒ | | | | ☒ | ☒ |

**EQUALITY AND DIVERSITY**

This policy has been written and reviewed with due regard to the legal duties set out in the Equality Act 2010, to ensure that no member of our school community suffers discrimination or disadvantage regardless of age, race, gender reassignment, disability, civil partnership, religion and belief (or lack of belief), pregnancy and maternity, gender or sexual orientation.

**Acknowledgements**

This policy is based on the SWGfL Online Safety Policy and Acceptable Use Agreements.
DFE Cloud Software Services and the Data Protection Act.
DFE Safeguarding Children and Young People from Sexual Exploitation.

Adopted: November 2020 Lorna Wilby
Review date: November 2021

**Appendix 1**

# Our Lady's Catholic Primary School
# Acceptable Use Agreement: Pupils

This agreement is intended to ensure:
• That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
• That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

- I understand that I must use school computing systems in a responsible way.
- I will only use computing systems in school for school purposes.
- I will take care of the computers and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will only open/delete my own files.
- I will only use my school e-mail address for educational purposes.
- I will only open e-mail attachments from people I know or that my teacher has approved.
- I will make sure that all contact with other children and adults is responsible and polite.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not tell other people my passwords.
- I will not give out my own details such as my name, phone number or home address.
- I will not install or uninstall programmes of any type on any school device, nor will I try to alter computer settings without guidance.
- I should ensure that I have permission to use the original work of others in my own work.
- I know that my parent/carer will be contacted if there is a concern about my Online Safety.

_____Teacher signature on behalf of pupils

Adopted: November 2020 Lorna Wilby
Review date: November 2021

**Appendix 2**

# Our Lady's Catholic Primary School
# Acceptable Use Agreement: Parent/Carer

Dear Parent/Carer

Digital technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any technology.

The Pupil Acceptable Use Agreement is intended to ensure:

- That pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The Parent/Carer Acceptable Use Agreement:
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times.
- Be respectful of other parents/carers and children.
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure.

I will not:

- Use private groups, the school's Social Media pages, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way.
- Use private groups, the school's Social Media pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident.
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers.

A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that you are aware of the school expectations. Parents are requested to sign the permission form below to show their support of the school and agreement to the Parent/Carer acceptable Use Agreement

.....

I agree to the Parent/Carer Acceptable Use Agreement. I know that my child has discussed an Acceptable Use Agreement and has received, or will receive, Online Safety education.

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 computing systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Parent/Carer Signature ……
Child's name ……
Date ……

Adopted: November 2020 Lorna Wilby
Review date: November 2021

**Appendix 3**

# Our Lady's Catholic Primary School
## Acceptable Use Agreement: Staff, Governors and Visitors

Digital technologies (including the use of data) such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of technology. All staff are expected to sign this agreement and adhere to its content at all times.

- I will only use the school's internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Local Governing Board.
- I will not use school email accounts as a 'chat room'.
- I will not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, staff and parents/carers are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address to pupils.
- I will not make my social media profiles available to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the Principal.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- I will not deliberately browse, download, upload or distribute any material that could be considered offensive, illegal, discriminatory or upsetting.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Online Safety leader or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use work of others in my own work.
- I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of digital technologies.

I agree to follow this agreement and to support the safe and secure use of technology throughout the school.

Signature …… Date ……
Full Name ……(printed)
Job title ……

Adopted: November 2020 Lorna Wilby
Review date: November 2021