St Oswald’s Catholic Primary School  
Online Safety Policy



## 

## Contents

Monitoring and review procedures

Roles and responsibilities

Policy Statements and Procedures

Communications and Remote learning

Mobile technologies

Use of Digital Images

Data Protection

Unsuitable / inappropriate activities

Illegal incidents

Staff Acceptable Use Policy

SMART Rules

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 Safety behaviour that take place out of school.

## Development / Monitoring / Review of this Policy

4

This Online Safety Policy has been developed by a working group made up of:

* Headteacher
* Online Safety Coordinator
* Staff – including Teachers, Support Staff, Technical staff
* Governors

Consultation with the whole school community has taken place through a range of formal and informal meetings.

## Schedule for Development / Monitoring / Review

5

|  |  |
| --- | --- |
| This Online Safety Policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on: |  |
| The implementation of this Online Safety Policy will be monitored by the: | Online Safety Coordinator / Senior Leadership Team |
| Monitoring will take place at regular intervals: | Annually |
| The 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) at regular intervals: | 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: | Autumn term 2021 |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | DSL, LADO, Police |

The school will monitor the impact of the policy using:

* Logs of reported incidents
* Monitoring logs of internet activity (filtering through Netsweeper systems inc. and a managed by LANCS ICT)
* Internal monitoring data for network activity
* Surveys / questionnaires of
  + pupils
  + parents / carers
  + staff

## Roles and Responsibilities

7

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

## Governors: Online Safety Governor (Mrs Sue O’Neill)

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 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 Governor. The role of the Online Safety Governor will include:

* regular meetings with the Online Safety Co-ordinator
* regular monitoring of online safety incident logs
* regular monitoring of filtering system
* reporting to relevant Governors

## Headteacher and Senior Leaders: (Mrs B Wood, Mr J Mears, Mr J Campbell)

* The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
* The Headteacher and the SLT will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
* The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. (Governor training and 360safe training for school staff)
* The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

## Online Safety Co-ordinator : (Mr J Campbell)

* leads the Online Safety and Digital leaders pupil group
* 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
* liaises with school technical staff (Western Business Systems)
* receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
* meets regularly with Online Safety Governor to discuss current issues, review incident logs and monitor the filtering system
* attends relevant Governors meetings
* reports termly to Senior Leadership Team

All online safety incidents will be dealt with in line with the school’s safeguarding policy and reporting procedures.

## Network Manager / Technical staff: Lancs ICT – Nigel Smith

The Network Manager is responsible for ensuring:

* that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
* that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply
* that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
* the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
* that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
* that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Online Safety Co-ordinator for investigation / action / sanction
* that monitoring software / systems are implemented and updated as agreed in school policies

## Teaching and Support 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 Staff Acceptable Use Policy Agreement (AUP)
* they report any suspected misuse or problem to the Headteacher / Online Safety Co-ordinator in line with Safeguarding policy
* online safety is regularly taught through age appropriate lessons which are embedded in all aspects of the computing,PSHE and RSE curriculum.
* pupils understand and follow the Online Safety S.M.A.R.T Rules (Safe, Meeting, Accepting, Reliable, Tell)
* pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
* in lessons where internet use is pre-planned 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. Open internet searches do not take place in lessons.

## Designated Safeguarding Lead and Deputy DSL.

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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

**Pupils**:

* are responsible for using the school digital technology systems in accordance with the Online Safety S.M.A.R.T Rules and Acceptable Use Policy (AUP)
* 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 (by telling an adult)
* will be expected to know and understand the rules on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-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 Rules 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. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at school events
* their children’s personal devices in the school

## Policy Statements – Procedures

## Education – Pupils

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

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

* A planned online safety curriculum is provided and is regularly revisited throughout the year based on the education for a connected world framework and Project Evole.
* Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
* Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
* Pupils are helped to understand the need for the online safety rules and encouraged to adopt safe and responsible use both within and outside school.
* Staff should act as good role models in their use of digital technologies the internet and mobile devices
* In lessons where internet use is pre-planned, it is best practice that pupils are 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, staff are vigilant in monitoring the content of the websites the young people visit.

## 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

* Letters, newsletters, website, blogs
* Parents / Carers evenings, remote Online safety training (National Online Safety)
* High profile events / campaigns e.g. Safer Internet Day
* Reference to the relevant web sites / publications

## Education & Training – Staff / Volunteers

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

A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

* All new staff receive the Online Safety Policy as part of their induction programme.
* All staff are asked to sign the Acceptable Use Agreements, ensuring that they fully understand acceptable use in school.
* The Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
* The Online Safety Co-ordinator will provide advice / guidance / training to individuals as required.

## Training – Governors

Governors should complete online safety training, (National Online Safety)

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.

## School technical systems

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

* There will be regular reviews and audits of the safety and security of school technical systems
* Servers, wireless systems and cabling must be securely located and physical access restricted
* All users will have clearly defined access rights to school technical systems and devices.
* The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place
* The Online coordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations and any licence issues will be reported to the Headteacher.
* Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider.
* Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
* The school has provided enhanced / differentiated user-level. All pupils are subject to strict filtering through the class logins.
* School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software, managed by Western Business Systems
* Guests (eg trainee teachers, supply teachers, visitors) will be granted limited access to the school system through a guest login.
* All school devices are used implicitly for school business and users are responsible for school devices outside of school (home)
* Staff cannot download any programmes or files to school systems and this is monitored through the filtering system. Any new software that is requested for installation is done so through the Administrator (Online Safety Co-ordinator)
* The use of removable media is limited to portable hard drives and USB sticks. These are password protected and encrypted.
* Personal data is not sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## Communications

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 | | | Pupils | | | | | |
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | | Allowed at certain times | Allowed with staff permission | Not allowed |
| \*Mobile phones may be brought to the school |  |  |  |  | |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  | |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  | |  |  |  |  |
| Taking photos on mobile phones |  |  |  |  | |  |  |  |  |
| Use of other mobile devices e.g. tablets, gaming devices |  |  |  |  | |  |  |  |  |
| Use of personal email addresses in school, or on school network (for communication) |  |  |  |  | |  |  |  |  |
| Use of school email for personal emails |  |  |  |  | |  |  |  |  |
| Use of messaging apps |  |  |  |  | |  |  |  |  |
| Use of social media |  |  |  |  | |  |  |  |  |
| Use of blogs |  |  |  |  | |  |  |  |  |

\*Children in year 6 can bring their mobile phone into school although it must be stored in the school office during school hours.

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

* The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
* Staff should therefore use only the school email service to communicate with others when in school.
* Pupils must immediately report to their class teacher or trusted adult in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* Staff to report to the Online Safety Co-ordinator in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* A link to the CEOP service is available on the school website for reporting any of the above.
* Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
* Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Remote Learning

* Remote (Home) learning is delivered through the school website with links to relevant resources.
* Conference calling software such as FaceTime, WhatsApp or Zoom is not used to communicate live with children or to provide ‘live lessons’ due to safeguarding considerations.
* As a school we do not have control over the content pupils will see on a conference call and therefore are unable to safeguard pupils from inappropriate or damaging material.

## Mobile Technologies

Mobile technology devices are supplied by the school. All users should understand that the primary purpose of the use mobile devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s Online Safety education scheme.

* The school Acceptable Use Agreements for staff, will give consideration to the use of mobile technologies

School owned devices:

* Allocated to classes (iPads / laptops)
* Used in school during school hours for educational purpose (not personal use)
* iPads have access to the school internet and purchased apps. Laptops have access to the school network through class logins.
* Management of devices overseen Online Safety Co-ordinator (including app purchases and device monitoring)
* Technical support provided by external technicians from Western business systems
* Internet access filtered through the Netsweeper filtering service provided by the local authority(BTSL).
* Access to cloud services is managed by class teachers only and monitored by the Computing Subject Leader / Online Safety Co-ordinator.
* Cameras and iPads are signed out of and returned to the school office, when they leave the premises on school trips.

**The school allows:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | | Personal Devices  **(including wearable technology)** | | |
|  | **School owned for single user (Staff)** | **School owned for multiple users** | **Student owned** | **Staff owned** | **Visitor owned** |
| Devices allowed in school | Yes | Yes | No \* | Yes | Yes |
| Full network access | Yes | Yes |  | No | No |
| Internet only |  |  |  | Yes | Yes  (on request) |

\*Children in year 6 can bring their mobile phone into school although it must be stored in the school office during school hours.

Personal devices:

* Personal devices are used in ‘Phone Zones’ during school hours. Personal devices are not permitted in all other areas of the school during school hours. (8.30am – 3.20pm)
* Student owned personal devices, including internet enabled wearable technology, are collected at the start of each day and stored in the school office. These are returned at the end of the school day. Pedometers (eg. Fitbits) are allowed.
* Personal devices can access the school internet but only outside of school hours or in designated ‘phone zones’.
* This network is restricted and password protected by the Netsweeper systems inc.
* Technical support is not available for personal devices
* Images are not be taken on personal devices.
* Visitors and Contractors are informed on arrival that the school is ‘Mobile device free’ and personal devices are only to be used in the permitted areas located around school. This is communicated via a poster in the school foyer.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

* When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
* Permission from parents or carers will be obtained at the beginning of every school year regarding the taking and publishing of children’s images (photos and videos.) Parents / Carers put in writing if they wish for their child’s image not to appear in any online school communication. (Website / YouTube Channel / Twitter)
* Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Pupils must not take, use, share, publish or distribute images of others without their permission
* Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
* Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

## Data Protection – See GDPR Policy

## Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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 / or outside the school when using school equipment or systems. The Online Safety Policy restricts usage as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User Actions  18 | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 |  |  |  |  | X |
| Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. |  |  |  |  | X |
| Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 |  |  |  |  | X |
| Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 |  |  |  |  | X |
| Pornography |  |  |  | X |  |
| Promotion of any kind of discrimination |  |  |  | X |  |
| threatening behaviour, including promotion of physical violence or mental harm |  |  |  | X |  |
| Promotion of extremism or terrorism |  |  |  | X |  |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | X |  |
| Using school systems to run a private business | |  |  |  | X |  |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | |  |  |  | X |  |
| Infringing copyright | |  |  |  | X |  |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | |  |  |  | X |  |
| Creating or propagating computer viruses or other harmful files | |  |  |  | X |  |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | |  |  |  | X |  |
| On-line gaming (educational) | | X |  |  |  |  |
| On-line gaming (non-educational) | |  | X |  |  |  |
| On-line gambling | |  |  |  | X |  |
| On-line shopping / commerce | |  |  | X |  |  |
| File sharing | | X |  |  |  |  |
| Use of social media | |  |  | X |  |  |
| Use of messaging apps | |  |  | X |  |  |
| Use of video broadcasting e.g. Youtube  19 | | X |  |  |  |  |

## Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.

## Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

#### For my professional and personal safety:

* I understand that the school will monitor my use of the school digital technology and communications systems.
* I understand that the rules set out in this agreement also apply to use of these technologies (e.g. school laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
* I understand that the school digital technology 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 understand that I should not write down or store a password where it is possible that someone may steal it.
* I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

28

#### I will be professional in my communications and actions when using school ICT systems:

* 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.
* I will only use social networking sites in school in accordance with the school’s policies.
* I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
* I will not engage in any online activity that may compromise my professional responsibilities.

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

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

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

* I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

