St Oswald's Catholic Primary School

Online Safety Policy

2025-2028

Approved by:	Approval date	Renewal date
Full Governors	4th December 2025	Autumn 2028

This Online Safety policy is set within the context of the whole school aims and mission statement:

Together with Jesus,
We will Learn and Grow in Faith

Statement of policy

'Our school is committed to safeguarding children and promoting children's welfare and expects all staff, governors, volunteers and visitors to share this commitment and maintain a vigilant and safe environment. Everyone has a responsibility to act without delay to protect children by reporting anything that might suggest a child is being abused or neglected. It is our willingness to work safely and challenge inappropriate behaviours that underpins this commitment. The school seeks to work in partnership with families and other agencies to improve the outcomes for children who are vulnerable or in need"

Our school aims to:
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Strategic and operational practices

At this school:

- The Head Teacher, Donna Hay, is the Senior Information Risk Officer (SIRO).
- Mr Strom is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners in a spreadsheet, located on the admin shared drive.
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as

when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.

- All staff are DBS checked and records are held in one central record – located on the admin confidential shared drive. We ensure ALL the following school stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed.
- staff
- governors
- pupils
- parents
- volunteers
- This makes clear all responsibilities and expectations with regard to data security.
- We have approved educational web filtering across our wired and wireless networks.
  We monitor school e-mails / blogs / online platforms, etc. to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.
- We follow LA guidelines for the transfer of any data, such as SIMS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use STRONG passwords for access into our SIM system.
- We require staff to change their passwords into the MIS, USO admin site, other secure system every 90 days / twice a year.
- We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff who set up usernames and passwords for e-mail, network access, and other online services work within the approved system and follow the security processes required by those systems.

- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use G-Suite for Education for online document storage.
- We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use Micro-soft Azure online Backup for disaster recovery on our <network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a cross-cut shredder.

Online Safeguarding Guidance

Use of technology for online / virtual teaching

All staff at St. Oswald's Catholic Primary school use Google Classrooms for online / virtual teaching or Class Dojo for EYFS; this has been agreed by all stakeholders for its appropriate level of security. Wherever possible, staff should use school devices and contact pupils only via the pupil school email

address / log in. This ensures that the setting's filtering and monitoring software is enabled.
Virtual lessons should be timetabled and senior staff, should be able to drop in to any virtual lesson at any time – the online version of entering a classroom. Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents. The following points should be considered:
▪ think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
▪ staff and pupils should be in living / communal areas – no bedrooms
▪ filters at a child's home may be set at a threshold which is different to the school
▪ resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content. (*Reference to Remote learning policy*).

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary
Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required.
If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details. All parental contact is recorded on CPOMS and SLT notified.

Educating pupils about online safety

In **EYFS & Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Understand the impact of their digital footprint

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or over Google Classroom/Class Dojo/Arbor. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the Senior Leadership team.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyberbullying

Definition: *Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.* (See also the school behaviour policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes RSHE education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on safe internet use and online safeguarding issues including cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy
Behaviour policy
Staff disciplinary procedures
Data protection policy and privacy notices
Complaints procedure
Computing policy
Safe Use of AI Policy