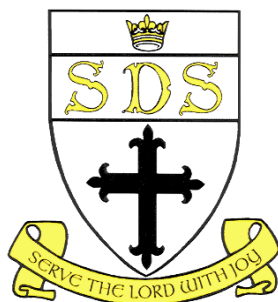
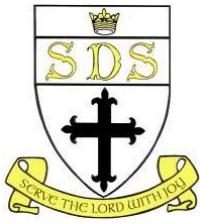


ST DOMINIC SAVIO CATHOLIC PRIMARY SCHOOL



Name of Policy:	Online Safety Policy
Date Adopted:	2 nd October 2025
Responsible Person:	Headteacher
Approval:	FGB
Review Date:	Autumn 2026
Signed By:	Laura Hulland Headteacher
Signature:	
Date:	2 nd October 2025
Signed By:	Fiona Cottle Chair of Governing Body
Signature:	
Date:	2 nd October 2025

[illegible]



ST DOMINIC SAVIO CATHOLIC PRIMARY SCHOOL

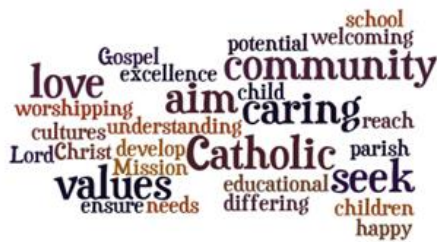
Commitment to equality:

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation. We have developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies are reviewed regularly in this regard.



Our Mission Statement

SERVE THE LORD WITH JOY



**We love Jesus and the Gospel values
inspire and guide us.**

**Happy, welcoming, worshipping and caring
community is who we are.**

**We fulfil each child's potential, developing
tomorrow's talent, today!**

Home, parish and school working together.

We are all God's children and respect everyone.



*"To welcome this little child in my name is to
welcome me; and to welcome me is to
welcome Him who sent me."*

(Luke 9:48)

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 or smart watches)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.1. The 4 key categories of risk

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

2. Roles and Responsibilities

2.1 Governors

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Mr Gunter Kuhnle (Safeguarding Governor)

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

2.2 Headteacher and Designated Safeguarding Lead– Mrs Laura Hulland

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety Liaising with other agencies and/or external services if necessary
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Develop understanding, policies and procedures in line with emerging [DfE guidance on the use of Generative AI](#) which is used to support school to use generative artificial intelligence safely including how filtering and monitoring requirements apply to the use of generative AI in education.

2.3 The ICT Technician (Mrs Michele Miller) and ICT Support (Tom Waterman)

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

2.4 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by using safeguarding reporting processes (see safeguarding policy).
- Following the correct procedures by if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy and our safeguarding policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

2.5 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

3. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#).

We also follow the curriculum set out by 'Education for a Connected World'.

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- [Relationships education and health education](#) in primary schools

In **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

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 Special Educational Needs.

4. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website.

Online safety will also be covered during parents' evenings, where appropriate.

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

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

5. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. The school defines as 'Several Times on Purpose' STOP (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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. Class teachers will discuss cyber-bullying with their year groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on 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/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
 - Is identified in the school rules as a banned item for which a search can be carried out, and/or
-

- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carers refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices in school

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school in writing.
- As per our uniform policy, no smart watches are allowed in any circumstances.
- Where mobile phones are allowed in school they will be switched off and stored in the school office during school time. The sending of abusive or inappropriate messages or images is forbidden.
- Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. From September 2027, no smartphones will be allowed in school.

Any breach of the acceptable use agreement by a pupil will be dealt with in line with the school behaviour policy, which may result in the confiscation of their device.

8.1 Staff using mobile devices in school

- Staff should not use their mobile phones in communal areas such as corridors or classrooms.
- Staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.

Staff must use their mobile phone in line with the acceptable use agreement. Any breach of this may result in disciplinary action.

9.0 Staff using work devices outside of school

Staff laptops are likely to be taken out of school and may well contain sensitive data.

The following security measures should also be taken with staff laptop/devices:

- Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
 - Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
 - Laptops/devices should never be left in a parked car, even in the boot.
 - Screensavers should be set to lock after a maximum of 15 minutes.
 - Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
 - Staff laptops should not be used by family members or pupils.
 - Work devices must be used solely for work activities.
-

10.0 Social networking

For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, X, blogs, online gaming, YouTube, WhatsApp, Snapchat, Instagram etc.

- Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- Pupil use of social networking should conform to age restrictions and will not be allowed in school.

10.1 Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a 'private' online space.

10.2 Access to social networking sites

- Social networking sites should never be accessed during contact time with pupils.
- Staff may not use school equipment to access social networking sites.
- If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.

10.3 Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, are unnamed and only posted with parental permission.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

10.4 Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents simply because they teach their children.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

11.0 Internet usage

- Pupils and staff will be informed that internet access can be monitored by staff and governors at any time.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Unauthorised users must not attempt to disable or reconfigure any filtering, virus protection or similar.

- All pupils using the internet, and associated communication technologies, will be made aware of the school's Online Safety Guidelines. These should be posted near to the computer systems.
- Pupils will receive guidance in responsible and safe use on a half termly basis.

12.0 Digital and video images

Staff must only use school equipment to take photos of children unless given specific authorisation by the Head Teacher. The use of cameras on mobile phones or the downloading of images onto any internet site is forbidden.

12.1 Parents or Members of the Public

The school understand that parents like to take photos of or video record their children in the school production, or at sports day, or school presentations. This is a normal part of family life, and we will not discourage parents from celebrating their child's successes. Where photographs are taken at an event attended by large crowds, this is regarded as a public area so it is not necessary to get permission of everyone in a crowd shot. The Data Protection Act does not apply to photographs or films taken for personal use by family and friends.

Parents will be asked to keep all images for their own use and not share on social media.

The school will not allow images of pupils to be used on school websites publicity, or press releases, including social networking sites, without permission from the parent, and if we do obtain such permission, we will not identify individual children by their full name.

Where a commercial photographer is used at a school event, the school will follow the NSPCC guidelines which are as follows:

- Schools should provide a clear brief about what is considered appropriate in terms of content and behaviour;
- Schools should issue the photographer with identification which must be worn at all times;
- Schools should let parents and children know that a photographer will be in attendance at an event and ensure they consent to both the taking and publication of films and photographs;
- Schools should not allow unsupervised access to children;
- Schools should not approve / allow photo sessions outside the event or at a child's home.

If children or parents have any concerns about inappropriate or intrusive photography, they should report them to the Child Protection Officer who would report them in the same manner as any other child protection concern.

If schools or parents have concerns regarding the use of filmed images by television companies they should contact the Office of Communication (Ofcom). Any objections to this policy should be addressed to the Child Protection Officer.

13. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with

the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, weekly briefings and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
 - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13.0 Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

The following are included in the appendices:

- Pupil Acceptable Use Agreement (KS1 and KS2)
 - Mobile Phone Use Agreement (for those bringing devices to school)
 - Parent/Carer Acceptable Use Agreement
 - Laptop Acceptable Use Agreement
 - Staff Acceptable Use Agreement
-

Pupil Acceptable Use Agreement

For my own personal safety:

- I understand that the school will monitor my use of the Computing systems and any digital communications.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will not communicate with anyone I don't know online.
- I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online.
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school Computing systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

Acting as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

Keeping secure and safe when using technology in school:

- Mobile phones will be handed into the school office for safe storage during the school day. Permission for the phone to be in school should be given in writing by a parent/carer and we will both sign the acceptable use agreement for mobile phones.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should 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 try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

I have read and understood the above and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

St Dominic Savio Catholic Primary School Mobile Phone Permission Form and Acceptable Use Agreement

This form must be completed by anyone child who seeks permission to bring their mobile phone to school.

1. You must have permission from your parent and your teacher to bring your phone to school. This may be because you have been allowed to walk to and from school without an adult.
2. On entry to the school grounds, phones must be switched off (not just put on 'silent'). Phones then need to be placed out of sight such as in a school bag.
3. You must comply with a request by a member of staff to switch off, or hand over, a phone.
4. Mobile phones must be immediately handed into the appropriate staff member in your year group.
5. You cannot take photos or recordings (either video or audio) of school staff or other pupils on school site. You must not take photos or recordings school staff or other pupils off site without consent.
6. Avoid sharing your contact details with people you don't know, and don't share other people's contact details without their consent.
7. Ensure your phone's password(s) or access code(s) are kept private from anyone else. You are responsible for your own phone.
8. Use your mobile phone responsibly at all times and refrain from using technology to bully, intimidate or harass anyone.
9. When using your phone, make sure that it is not used to send or receive which could be considered criminal. For instance, by sending inappropriate messages or images.
10. Rules on bullying, harassment and intimidation apply to how you use your mobile phone even when you aren't in school.
11. When using your phone or social media, ensure the language used is at all times appropriate.
12. Make a conscious effort to avoid viewing and/or sharing harmful or dangerous content.
13. Phones are not permitted on school trips or any school event, including school discos.
14. At the end of the school day, your phone will be returned to you. You are not permitted to turn the phone back on until you leave the school premises. If you need to make a call on the school site, please alert a member of staff.

Pupil name:	
Year group/class:	
I understand that to bring my phone to school, I must follow the rules above:	
Signed by Pupil:	Date:
I support the school in ensuring my child follows this agreement.	
Signed by Parent:	Date:
I give permission for this child to bring their phone to school if they follow this policy.	
Signed by teacher:	Date:

Parent/Carer Acceptable Use Agreement (Key Stage 1)

The school seeks to ensure that pupils have good access to Computing to enhance their learning and, in return, expects pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

=====

Acceptance of Use Form

Parent/Carer's Name:	
Pupil's Name:	

As the parent/carers of the above pupil, I understand that my son/daughter will have access to the internet and to Computing systems at school.

I know that my son/daughter has received, or will receive, Online Safety education to help them understand the importance of safe use of Computing – 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 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.

I understand that my son's/daughter's activity on the Computing 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 Online Safety.

I have read and understood the school's online safety policy.

Signature:	
Date:	

Parent/Carer Acceptable Use Agreement (Key Stage 2)

The school seeks to ensure that pupils have good access to Computing to enhance their learning and, in return, expects pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

=====

Acceptance of Use Form

Parent/Carer's Name:	
Pupil's Name:	

As the parent/carers of the above pupil, I understand that my son/daughter will have access to the internet and to Computing systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of Computing – 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 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.

I understand that my son's/daughter's activity on the Computing 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 Online Safety.

I have read and understood the school's online safety policy.

Signature:	
Date:	

Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

- I understand that it is a criminal offence to use a school Computing system for a purpose not permitted by its owner.
- I appreciate that Computing includes a wide range of systems, including mobile phones, e-mail, social networking and that Computing use may also include personal Computing devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including e-mail and social networking) and any comments on the web are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the internet is consistent with the school's Online Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding pupils' safety to the DSL – Mrs Laura Hulland.

Mobile phones/personal devices

- I will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures.
- I will not use my mobile phone in front of the children.
- I will store my phone/device in a secure place during lesson time and ensure that it is on 'silent mode'.
- I will not use it take any photographs or videos of children (except in exceptional circumstances with permission of the headteacher).
- I will not send photos or videos of children using my personal device.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place.

Name:	
Signature:	
Date:	

Laptop/Devices Acceptable Use Agreement

1. Introduction

- This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
- It should be read in conjunction with the school's Online Safety Policy
- All recipients and users of these devices should read and sign the agreement.

2. Security of equipment and data

- The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
- Staff should understand the limitations of the school's insurance cover.
- Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

3. Software

- Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
- Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
- Users should not attempt to make changes to the software and settings that might adversely affect its use.

4. Faults

- In the event of a problem with the computer, the school's Computing Technician/Network Manager should be contacted.

5. Return of laptop / device

- Any laptop / device should be returned to the Computing Technician/Network Manager on the last day in school when a member of staff is leaving the employment of the school or starting maternity leave. In the event of long term sick leave the laptop / device should be returned as soon as practicable.

Declaration:

I have read and understood the above and also the school's Online Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	
