Christ Church CE VC Primary School

“Together we learn - Together we grow - Together we flourish”

Some seeds fell on good earth and produced a harvest beyond wildest dreams.

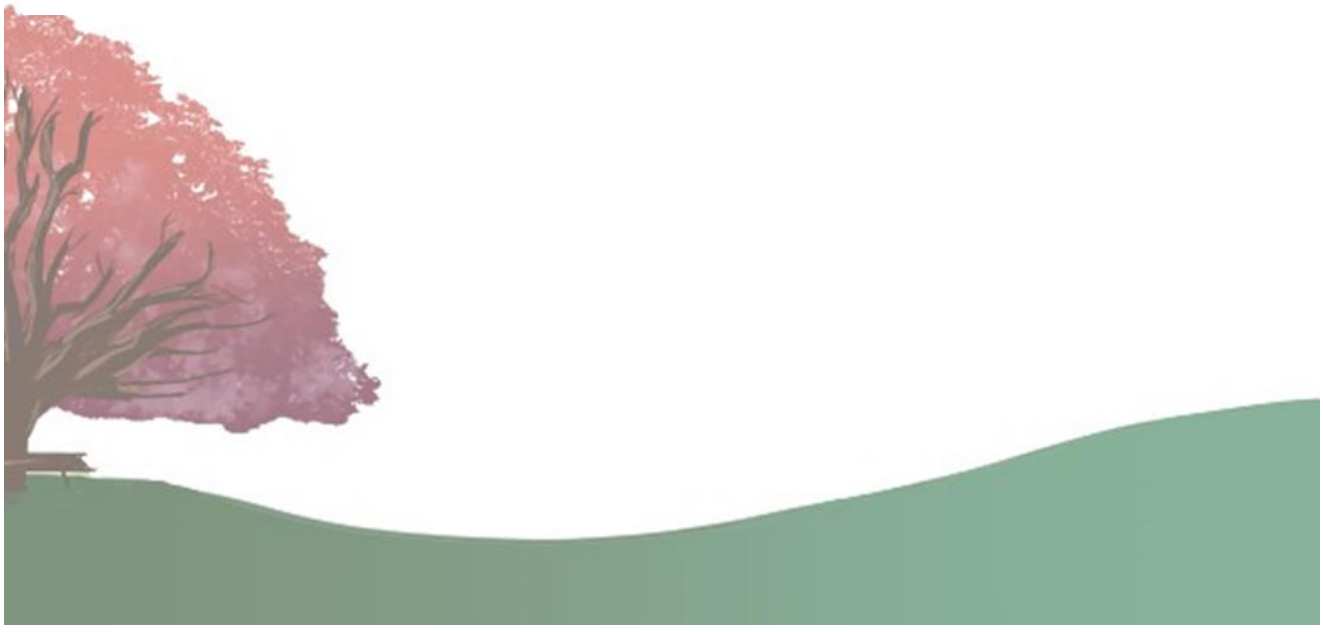
Matthew 13:8

Online Safety Policy

Date ratified:

Ratified by:

Review date:



1. Aims

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.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content –** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact –** being subjected to harmful online interaction with other users, such as 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 –** personal online behaviour that increases the likelihood of, or causes, harm, such as 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

2. 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
- [Relationships and sex education
- 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.

3. Roles and responsibilities

3.1 The whole school community

In addition to the roles and responsibilities outlined below, and to support the implementation of this policy, the school has compiled acceptable use agreements, which provide clear guidance in relevant areas such as conduct, access and use of the school system, removable media, downloading files, sharing information, social networks and devices (both school and personal equipment within and outside school).

Separate agreements have been written for the groups below who are all expected to read and sign them to acknowledge their responsibilities in this area:

- staff and volunteers
- parents
- pupils

We also ask that parents help to support the school in ensuring that their children understand their responsibilities and roles in online safety.

3.2 The governing board

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

All governors will:

- Ensure that 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 (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college 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

The Safeguarding, Wellbeing and Inclusion Committee (SWIC) will have specific oversight of online safety and the online safety policy and will report on its implementation to the Full Governing Body.

The SWIC will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL) and the deputy designated safeguarding leads (DDSLs).

3.3 The headteacher

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

The headteacher is responsible for ensuring that the DDSL who leads on online safety is given suitable training and support to enable them to carry out their online safety roles and to train other colleagues as required.

3.4 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies (DDSLs) are set out in our safeguarding policy as well as relevant job descriptions.

The DSL and DDSLs take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Taking day to day responsibility for online safety policies and procedures and a leading role in reviewing the school's online safety policies and procedures.
- Working with the headteacher, 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 safeguarding 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 (appendix 4 contains a self-audit for staff on online safety training needs) and ensuring staff are all aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Liaising with other agencies and/or external services if necessary.
- Liasing with the school's technical support and external providers.
- Providing regular reports on online safety in school to the SWIC and governing board.

This list is not intended to be exhaustive.

3.5 Network Manager

The school's managed ICT Service is provided by an outside contractor; however it remains the responsibility of the school to ensure that the appointed contractor carries out all the required online safety measures and is fully aware of the school's policy. These include:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (via CPOMs) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Regularly monitoring the use of the network/internet/Learning Platform/remote access/ email in order that any misuse or attempted misuse can be reported to the DSL/ DDSLs for investigation and any subsequent action that might be required.

This list is not intended to be exhaustive.

3.6 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged (via CPOMs) and dealt with appropriately in line with this 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'.
- Ensuring online safety issues are embedded in all aspects of the curriculum and other activities

- Ensuring pupils understand and follow the online safety policy and acceptable use agreement.
- In lessons where internet use is pre-planned, guiding pupils to sites checked as suitable for their use and ensuring that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Monitoring 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.

This list is not intended to be exhaustive.

3.7 Parents

Parents 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 (appendices 1 and 2)
- Support their children to understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through:
  - parents' evenings.
  - newsletters and letters.
  - the school's website and learning platform.
  - information about national and local online safety campaigns.
- 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.
  - access to parents' sections of the website/learning platform and online pupil records.
  - their children's personal devices in the school (where this is allowed).

Parents 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

3.7 Pupils

Pupils are responsible for using the school's digital technology systems in accordance with the 'Pupil Acceptable Use Agreement' and:

- will be expected to know and understand the school's rules on the use of mobile devices and digital cameras including the taking of and use of images and on cyber-bullying.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, and.
- 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.

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

All primary schools have to teach: Relationships education and health education

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 SEND.

5. 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. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

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

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

6. 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. (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.

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 (see section 11 for more detail).

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 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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. Pupils are to submit their device to their class teacher on arrival, for it to be kept in a secure location during the school day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 2).

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

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- 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)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

If staff have any concerns over the security of their device, they must seek advice from the DSL/ DDSL.

10. Communication and content

10.1 Website content (please also refer to the section on the use of digital and video images below)

- The point of contact on the school website is the school address, school e-mail and telephone number. Staff or pupils' personal information is not published.
- The headteacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- The website complies with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Where audio and video are included (e.g. podcasts and video blogging) the nature of the items uploaded does not include content that allows the children to be identified.

10.2 Learning Platforms

- An effective learning platform (LP) or virtual learning environment (VLE) offers a wide range of benefits to teachers, pupils and parents, as well as support for management and administration.
- All users will be required to use an age appropriate password to access the relevant content of the LP which must not be shared with others.
- The DSL and DDSLs will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils, staff and parents will be advised about acceptable conduct and use when using the LP and this shall be included in parent and pupil user agreements.
- Only members of the current pupil, parent and staff community will have access to the LP.
- All users will be mindful of individual and intellectual property and will upload only appropriate content to the LP.
- When a user leaves the school their account or rights to relevant content areas will be disabled or transferred to their new establishment.

10.3 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 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, pupils will be educated and informed 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.

- In accordance with guidance from the Information Commissioner's Office (ICO), parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images. This is clearly laid out in the acceptable use agreement for parents.

- Staff and volunteers are allowed to take digital /video images to support educational aims, but must follow the 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.

- The school will comply with the Data Protection Act and request parents' permission before taking images of members of the school and also ensure that when images are published by the school (e.g. on the website, in newsletters or in print) that pupils cannot be identified by the use of their full names.

- Photographs published on the school website, or elsewhere, that include pupils will be carefully selected and will comply with good practice guidance on the use of such images.

- Care will 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.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

10.4 On line communications and social media

- The official school email service may be regarded as safe and secure and is monitored. All users should be aware that email communications are monitored.

- Users must immediately report to the headteacher, in accordance with the school's 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 communications.

- Any digital communication between staff and pupils or their parents (email, social media, chat, blogs, remote learning platform etc.) must be professional in tone and content and should only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Any digital communication relating to the school which takes place between users (email, social media, chat, blogs, remote learning platform etc.) must be professional in tone and content and may only take place on the official monitored school system. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils may only use approved email accounts on the school system and must not access any external personal email accounts from any school computer.

- Pupils will not be issued with individual email accounts, but may be authorised to use a class email address under supervision.

- Emails sent to any external organisations should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the DSL/ DDSLs before using social media tools in the classroom.

- All staff should be familiar with the 'Acceptable Use Agreement' and with the school's Code of Conduct in relation to the use of social media, in particular they should:

o have a clear understanding of reporting guidance, including their responsibilities, the procedures that they must follow and the sanctions that might apply in the event of any departure from those procedures.

o ensure that no reference is made in social media to pupils, parents or other members of the school staff and that they do not used social media platforms to discuss any personal matters relating the school community.

o not use any personal social media accounts to communicate in a way that has any impact on the school or associate their comment with the school as, should this be the case, such personal communication are within the scope of this policy.

o not publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.

o must not harass, engage in online bullying, discriminate on the grounds of sex, race and/or disability or who defame a third party may render the school liable, and

- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents, particularly when concerning underage use of sites.

10.5 Official school social media accounts

In the case of official social media accounts established by the school, there should be:

- a clear process for approval by senior leaders.

- a clear process for the administration and monitoring of these accounts, involving at least two members of staff.

- a code of behaviour for users of the accounts including systems for reporting and dealing with abuse and misuse, and an understanding of how any such incidents may be dealt with under the schools disciplinary procedures.

10.6 Video Conferencing

Video conferencing (including FaceTime, Skype, Zoom and Teams) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

- If pupils engage in video conferencing, as part of the curriculum, this will be supervised at all times

11. 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 ICT 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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12. 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, e-bulletins 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 DDSLs 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 safeguarding policy.

13. Monitoring arrangements

Staff report behavior and safeguarding issues related to online safety via CPOMs. The DSL and DDSLs use CPOMs to respond and monitor incidents.

This policy will be reviewed every year by the SWIC and the DSL/ DDSLs At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Wilts Staff Behaviour Policy
- Code of Conduct

- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable Use Agreement (Parents/Carers of EYFS and KS1)

Via Microsoft Forms

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS.

Please read each statement aloud to your child and click the 'I have discussed this with my child' box.
You will need to complete a separate form for each individual child.
* Required

1. My EYFS/KS1 child's name and class is:

(Please include first name **only** and your child's class. E.g. Bob, Owls.) *

2. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **I will ask my teacher or a school adult if I can do so before using them.** *

◯ I have discussed this with my child

3. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **I will only use websites that my teacher or adult has told me or allowed me to use.** *

◯ I have discussed this with my child

4. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **I will tell my teacher immediately if:**

I click on
I receive
I find

- **a website by mistake**
- **messages from people I don't know**
- **anything that may upset or harm me or my friends**

*

◯ I have discussed this with my child

5. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **I will use school computers for school work only.** *

◯ I have discussed this with my child

6. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **I will be kind to others and not upset or be rude to them.** *

◯ I have discussed this with my child

7.
I will look after the school computing equipment and tell a teacher straight away if something is broken or not working properly. *

◯ I have discussed this with my child

8. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **if I have any usernames and passwords, I will:**

- **Only use the username and password I have been given**
- **Try my hardest to remember my username and password**
- **Never share my password with anyone, including my friends** *

◯ I have discussed this with my child

9. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **I will never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.** *

◯ I have discussed this with my child

10. When I use the school's ICT systems (for example, computers or iPads) and get onto the internet in school, **I will check with my teacher before I print anything.** *

◯ I have discussed this with my child

11. **I will log off or shut down a computer when I have finished using it.** *

◯ I have discussed this with my child

12. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** *

◯ My child agrees

13. (For parents/carers) **I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.** *

◯ I agree

Appendix 2: Acceptable Use Agreement (pupils and parents/carers of KS2) Via Microsoft Forms

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS.

Please read each statement aloud to your child and click the 'I have discussed this with my child' box.

You will need to complete a separate form for each individual child.

* Required

1. My KS2 child's name and class is:
(Please include first name **only** and your child's class. E.g. Bob, 4GA) *

2. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will always use the school's ICT systems and the internet responsibly and for educational purposes only.** *

◯ I have discussed this with my child

3. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will only use them when a teacher is present, or with a teacher's permission.** *

◯ I have discussed this with my child

4. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will keep my usernames and passwords safe and not share these with others.** *

◯ I have discussed this with my child

5. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer.** *

◯ I have discussed this with my child

6. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will tell a teacher or LSA immediately if I find any material which might upset, distress or harm me or others.** *

◯ I have discussed this with my child

7. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will always log off or shut down a computer when I've finished working on it.** *

◯ I have discussed this with my child

8. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will not access any inappropriate websites, including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.** *

◯ I have discussed this with my child

9. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will not use any inappropriate language when communicating online (including in emails).** *

◯ I have discussed this with my child

10. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will not create or share any material that is offensive or inappropriate.** * ◯ I have discussed this with my child

11. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will not log in using someone else's details.** *

◯ I have discussed this with my child

12. When I use the school's ICT systems (like iPads or computers) and get onto the internet in school, **I will not arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.** *

◯ I have discussed this with my child

13. **When I am in year 6, if I bring a personal mobile phone or other personal electronic device into school, I will not use it during the school day and give it in to my teacher to store securely.** *

◯ I have discussed this with my child

14. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** *

◯ My child agrees

15. (For parents/carers)

- **I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.**
- **I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.**

*

◯ I agree

Appendix 3: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

Via Microsoft Forms

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

1. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not access, or attempt to access, inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).** *

◯ I agree

2. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not use them in any way which could harm the school's reputation.** *

◯ I agree

3. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not access social networking sites or chat rooms.** *

◯ I agree

4. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not use any improper language when communicating online, including in emails or other messaging services.** *

◯ I agree

5. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not install any unauthorised software, or connect unauthorised hardware or devices to the school's network.** *

◯ I agree

6. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not share my password with others or log in to the school's network using someone else's details.** *

◯ I agree

7. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not take photographs of pupils without checking with the class teacher first.** *

◯ I agree

◯ N/A (I am the class teacher)

8. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not share confidential information about the school, its pupils or staff, or other members of the community.** *

◯ I agree

9. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not access, modify or share data I'm not authorised to access, modify or share.** *

◯ I agree

10. When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I will not promote private businesses, unless that business is directly related to the school.** *

◯ I agree

11. I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. *

◯ I agree

12. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. *

◯ I agree

13. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. *

◯ I agree

14. I will report if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material, to the designated safeguarding lead (DSL) or one of the deputy designated safeguarding leads (DDSLs) using
CPOMs. *

◯ I agree

15. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. *

◯ I agree

Appendix 4: online safety training needs – self-audit for staff

Via Microsoft Forms

Self-audit for staff. You may add comments to your answers if necessary.

* Required

1. Do you know the name of the person who has lead responsibility for online safety in school? *

- [ ] Yes
- [ ] No
- [ ] Comments:

2. Are you aware of the ways pupils can abuse their peers online? *

- [ ] Yes
- [ ] No
- [ ] Comments:

3. Do you know what you must do if a pupil approaches you with a concern or issue? *

- [ ] Yes
- [ ] No
- [ ] Comments:

4. Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? *

- [ ] Yes
- [ ] No
- [ ] Comments:

5. Are you familiar with the school's acceptable use agreement for pupils and parents? *

- [ ] Yes
- [ ] No
- [ ] Comments:

6. Do you regularly change your password for accessing the school's ICT systems? *

- [ ] Yes
- [ ] No
- [ ] Comments:

7. Are you familiar with the school's approach to tackling bullying, including cyber-bullying? *

- [ ] Yes
- [ ] No
- [ ] Comments:

8. Are there any areas of online safety in which you would like training/further training? *