Dr Walker's C of E Primary School

An Exceptional Place to Flourish

Though your beginning was small,
your future will flourish indeed.
Job 8:7

STATUTORY POLICY

Online Safety Policy

Ratified by Governors	**02.10.2023**
Review Cycle	**Annually**

Chair of Governors: Mrs K Bush	
Headteacher: Dr L Lawson	

Contents

Pre-amble: School Vision, Ethos and Values

Dr Walker's is a mixed Church of England Voluntary Controlled Primary School in Fyfield, Ongar, Essex.

We support all pupils to succeed in reaching their God given potential at Dr Walker's – 'An Exceptional Place to Flourish', by developing

- **Belief** in self and the development of confidence, respect and trust for others and an appreciation of spirituality and an understanding of faith in God;
- **Engagement** in a love for learning by nurturing curiosity and independence; and
- **Excellence** in reaching personal goals by demonstrating resilience and positive behaviour.

Our CHRISTIAN VALUES are reflected in:

- **Standing with COURAGE for what is right.**
- **Using CREATIVITY in problem solving and making life beautiful.**
- **Treating every person and everything with RESPECT.**
- **Having COMPASSION for others.**
- **Completing every task with PERSEVERANCE.**
- **Taking RESPONSIBILITY for ourselves.**
- **Living with HOPE for a better future.**

At Dr Walker's we provide every pupil with the care and support they need to develop as individuals and become educated and successful British Citizens who understand the importance of the following British values:

- **Democracy**
- **The rule of law**
- **Individual liberty**
- **Mutual respect and**
- **Tolerance of those with different faiths and beliefs.**

Acknowledgement

Adopted from The Key's ***Model Online Safety Policy*** for schools.

This policy needs to be read in conjunction with other school polies:

- ***Child Protection Policy***
- ***Anti-bullying policy***
- ***Attendance Policy***
- ***Behaviour Policy***
- ***Equalities Policy***
- ***Harmful Sexual Behaviour Policy***
- ***SEND Policy***
- ***Whistleblowing Policy***

DESIGNATED SAFEGUARDING LEAD: (DSL)	**Dr Llewellen Lawson**
DEPUTY DESIGNATED SAFEGUARDING LEAD: (DDSL)	**Mrs Jenny Dean**
DEPUTY DESIGNATED SAFEGUARDING LEAD: (DDSL)	**Mrs Louise Morris**
DESIGNATED SAFEGUARDING GOVERNOR:	**Mrs Paulette Houghton**

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')
- 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.
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
  - PSHE/RSHE
  - 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 governing board	• 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.
		
		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 (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.

3.2	The Headteacher	• The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
3.3	The designated safeguarding lead	• Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

		The DSL takes 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. • Working with the headteacher and 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 • Working with the ICT manager to make sure the appropriate systems and processes are in place • 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's child protection policy. • Ensuring that any online safety incidents are logged (see appendix 5) 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). • Liaising with other agencies and/or external services if necessary. • Providing regular reports on online safety in school to the headteacher and/or governing board. • Undertaking annual risk assessments that consider and reflect the risks children face. • 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. This list is not intended to be exhaustive.
3.4	The ICT manager/ consultant	• 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 during visits to the school. • Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files. • Ensuring that any online safety incidents are logged (see appendix 5) 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. This list is not intended to be exhaustive.
3.5	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). • 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 informing the headtreacher and ICT manager/consultant. • Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes **(e.g. using the LGFL login to unblock sites such as www.youtube.co.uk using www.block.trustnet.pro).** • Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.' This list is not intended to be exhaustive.
3.6	**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 (appendices 1 and 2). 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
3.7	**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 schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary 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

Note:

- 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/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 and/or access to the online subscription of The National College and National Online safety (www.nationalcollege.com).
- Parents will also be signposted to the NSPCC www.nspcc.org.uk/keeping-children-safe/online-safety/).
- This policy will also be shared with parents/carers.
- Online safety will also be covered during parents' evenings.
- The school will let parents/carers 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/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.

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. Class teachers will discuss cyber-bullying with their tutor 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 (see section 11 for more detail).
- 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 DfE has published **"Screening, Searching and Confiscation"** guidance (2011), which the school will refer to if a pupil or group of pupils are suspected of being in possession of banned items or stolen goods.

- The headteacher, and any member of staff authorised to do so by the headteacher ***(as set out in the Behaviour Policy)*** 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.

- **The school is not required to inform parents before a search takes place and does not need to seek consent.**

- 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 / DSL / appropriate staff member.
  - 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/carer 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 (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 and restrict access through filtering systems where appropriate.
- More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

- Pupils are not allowed to bring in mobile phones to school.
- If they do bring a mobile phone to school it needs to be handed in at the office on arrival and collected at home time.
- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 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 that would violate the school's terms of acceptable use, as set out in appendix 3.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the ICT manager/consultant.

10. 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. 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 deputy/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.

12. Monitoring arrangements

- The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.
- This policy will be reviewed every year by the Governing Body.
- 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.

13. Links with other policies

This online safety policy is linked to our:

- ***Unacceptable and Abusive Behaviour Policy***
- ***Child protection and safeguarding policy***
- ***Behaviour policy***
- ***Staff disciplinary procedures***
- ***Data protection policy and privacy notices***
- ***Complaints procedure***
- ***ICT and internet acceptable use policy***

Appendix A - Abuse/bullying using cyber technology

Staff in schools may become targets of cyber abuse/bullying and, like other forms of bullying, it can have a significant impact on their health, well-being and self-confidence. Protecting staff from abuse is best done within a prevention framework, including whole school policies and appropriate practices.

Cyber abuse/bullying may consist of threats, harassment, embarrassment, humiliation, defamation or impersonation. It may take the form of general insults, or prejudice-based abuse, e.g. homophobic, sexist, racist or other forms of discrimination. It may involve email, virtual learning environments, chat rooms, websites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

Abuse using cyber technology can occur at any time and incidents can intrude into the victim's private life. The audience for such messages can be very large and can be reached rapidly. The content of electronically forwarded messages is hard to control and the worry of content resurfacing can make it difficult for the victim to move on.

The Governing Body endorses the decision of any school to operate a zero tolerance policy towards direct or indirect harassment or assault against any member of staff, volunteer, or member of the school community. This includes the use of social media and other forms of electronic communications to facilitate the act.

Cyberbullying and the law

While there is not a specific criminal offence called cyberbullying, activities can be criminal offences under a range of different laws, including:

- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988
- Section 127 of the Communications Act 2003
- Public Order Act 1986
- The Defamation Acts 1952 and 1996

It is the duty of every employer to ensure, so far as reasonably practicable, the health, safety and welfare at work of all employees. Incidents that are related to employment, even those taking place outside the hours or place of work may fall under the responsibility of the employer.

Effectively tackling abuse using cyber technology

- School behaviour policies and procedures should explicitly refer to and outline how the school will deal with cyber abuse/ bullying of both staff and pupils.
- They should include: rules on the use of equipment, software and network access provided by the school, the use of staff and pupil owned equipment and internet access routes, where they are used on school premises and within school hours, e.g. mobile phones, digital cameras and laptops acceptable behaviour including behaviour outside of school e.g. use of social networking services and other sites, regarding harming others and bringing the school into disrepute.

Appendix B - Responding to incidents

Staff should never retaliate i.e. personally engage with cyberbullying incidents.

- Keep any records of abuse – texts, emails, voice mails, or instant messages. Take screen prints of messages or web pages. Record the time, date and address of the site. This should be recorded on ScholarPack
- Inform the appropriate person e.g. headteacher, or head of year at the earliest opportunity.
- Where the perpetrator is known to be a current pupil, parent, or co-worker, this should be dealt with through the school's own behaviour management / disciplinary procedures.
- Monitoring and confiscation must be appropriate and proportionate - parents, employees and learners should be made aware in advance of any monitoring (for example, of email or internet use) or the circumstances under which confiscation might take place.
- A designated member of the leadership team should contact the police where it appears that a law has been broken – for example, where death threats, assault, or racially motivated criminal offences are involved. Where a potential criminal offence has been identified, the school should ensure that any internal investigation does not interfere with police inquiries. School staff are of course able to report incidents directly to the police.
- If a potential criminal offence has been committed and the school is not able to identify the perpetrator, the police may issue a Regulation of Investigatory Powers Act 2000 (RIPA) request to a service provider, enabling them to disclose the data about a message or the person sending it.

Essex legal services are available to offer support and advice.

Getting offensive content taken down

- Where online content is upsetting / inappropriate and the person(s) responsible for posting is known, the school will need to contact the host (i.e. the social networking site) to make a request to get the content taken down.
- The material posted may breach the service provider's terms and conditions of use and can then be removed.
- It is important to be clear about where the content is – for example by taking a screen capture of the material that includes the URL or web address.
- If you are requesting, they take down material that is not illegal, be clear how it contravenes the site's terms and conditions.
- In cases of actual/suspected illegal content, the school should contact the police.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

<table>
<tr><th colspan="2">ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends

• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• 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
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: 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.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like 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. • Only use them when a teacher is present, or with a teacher's permission. • Keep my usernames and passwords safe and not share these with others. • 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. • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others. • Always log off or shut down a computer when I've finished working on it. **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. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher. • Use any inappropriate language when communicating online, including in emails. • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate. • Log in to the school's network using someone else's details. • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision. **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission. • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: 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.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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) • Use them in any way which could harm the school's reputation. • Access social networking sites or chat rooms. • Use any improper language when communicating online, including in emails or other messaging services. • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network. • Share my password with others or log in to the school's network using someone else's details. • Take photographs of pupils without checking with teachers first. • Share confidential information about the school, its pupils or staff, or other members of the community. • Access, modify or share data I'm not authorised to access, modify or share. • Promote private businesses, unless that business is directly related to the school.	
• 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 that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • 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 will let the designated safeguarding lead (DSL) and ICT manager know 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. • I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

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

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**