St Cuthbert's C of E Primary School

The Chase, Great Glen, Leicester LE8 9EQ Tel: 0116 2592764

Online safety policy

Our Vision

Doing all the good we can, through faith, love and excellence.

Micah 6·8· "This is what the Lord requires of you: to do justice, and to love kindness and to walk humbly with your God."

We want St Cuthbert's to be a school where:

Our Ethos

- everyone flourishes through the guidance of our Christian values.
- teaching and learning is creative, engaging and motivational.
- relationships are positive and serve to support others through **compassion** and **kindness.**

"I have come that they may have life and have it to the full." John 10, V10

Our Expectations

- we show **courage** to be the best that we can be.
- the children make excellent progress, fostering a love of learning.
- every child has an **equal** chance to fulfil their full potential.

"All human kind is made in the image of God. " Genesis 1, V26-27

Individuality

- we grow and flourish as individuals; through **endurance** we can achieve.
- the value and worth of each individual is celebrated and everyone feels included.
- the children develop a spirit of **curiosity** and a willingness to rise to a challenge through a broad, enriched curriculum.

"All people are called to transform the world" Genesis 1 V26-31, Micah 6 V8

Working Together

- the children are able to **trust** show **respect** and **friendship** to others.
- the community enables our pupils and school to grow in a happy, safe, healthy and spiritual environment.
- we foster links and contribute to the educational community through effective communication.

"Every person is an individual and also part of a community." 1 Cor 12 V12-27

This is a vision that is inclusive to all as we are reminded in the words of Luke 18:16:
"But Jesus called them to him, saying, "Let the children come to me, and do not hinder them, for to such belongs the kingdom of God."
For we are all equal in the eyes of God.

Last reviewed on:	Oct 21
Next review due by:	Oct 23

Equal

“You shall love your neighbour as yourself.”

Mark 12:31

Potential

“Behold they are one people and they have all one language and this is only the beginning of what they will do.”

Genesis 11:6

Courage

“Be strong and courageous. Do not be frightened and do not be dismayed for the Lord your God is with you wherever you go.”

Joshua 1:9

Trust

“My God is my strength in whom I trust.”

Psalm 12

Friendship

“Encourage one another and build each other up.”

1 Thessalonians 5:11

Respect

“For God gave us a spirit not of fear but of power and love and self- control.”

Joshua 1:9

Endurance

“I can do all things through Him who strengthens”

Joshua 9

Contents

---

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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 Department'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 co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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)

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 DSL and deputies are set out in our child protection and safeguarding policy as well 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs (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

This list is not intended to be exhaustive.

3.4 The ICT Technician

The ICT Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 monthly 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 (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)
- 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

This list is not intended to be exhaustive.

3.6 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)

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 factsheet - Childnet International
- Parent guides on a range of internet safety concerns and guides for using apps -https://www.internetmatters.org/

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, during weekly computing lessons online safety will be covered each lesson to address all the concerns for their age group:

The text below is taken from the National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools

This new requirement includes aspects about online safety.

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

- 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. Safer internet day will be used to raise awareness of online safety as well as during computing lessons.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. Pupils will have the opportunity to discuss the different dangers online and strategies about how to protect themselves.

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 or communications system e.g parentmail, twitter This policy will also be shared with parents. Useful websites to support parents with protecting their children online will be shared and leaflets may be given out too to support parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the 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 one 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. Pupils will know that they can talk to any member of school staff and that their concern will be taken seriously. School staff will report any concerns on CPOMs which will alert the designated safeguarding leads.

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. Cyber bullying will be discussed as part of online safety during computing lessons, but it will also be covered in other areas of the curriculum such as PSHE especially if bullying is being mentioned. Class teachers will discuss cyber-bullying with their groups, and the issue will be addressed in assemblies.

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

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

8. Pupils using mobile devices in school

Pupils' who need to bring a mobile phone in to school can only do so if a written request is received from parents explaining the reason that a mobile phone would be needed.

Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

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

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician .

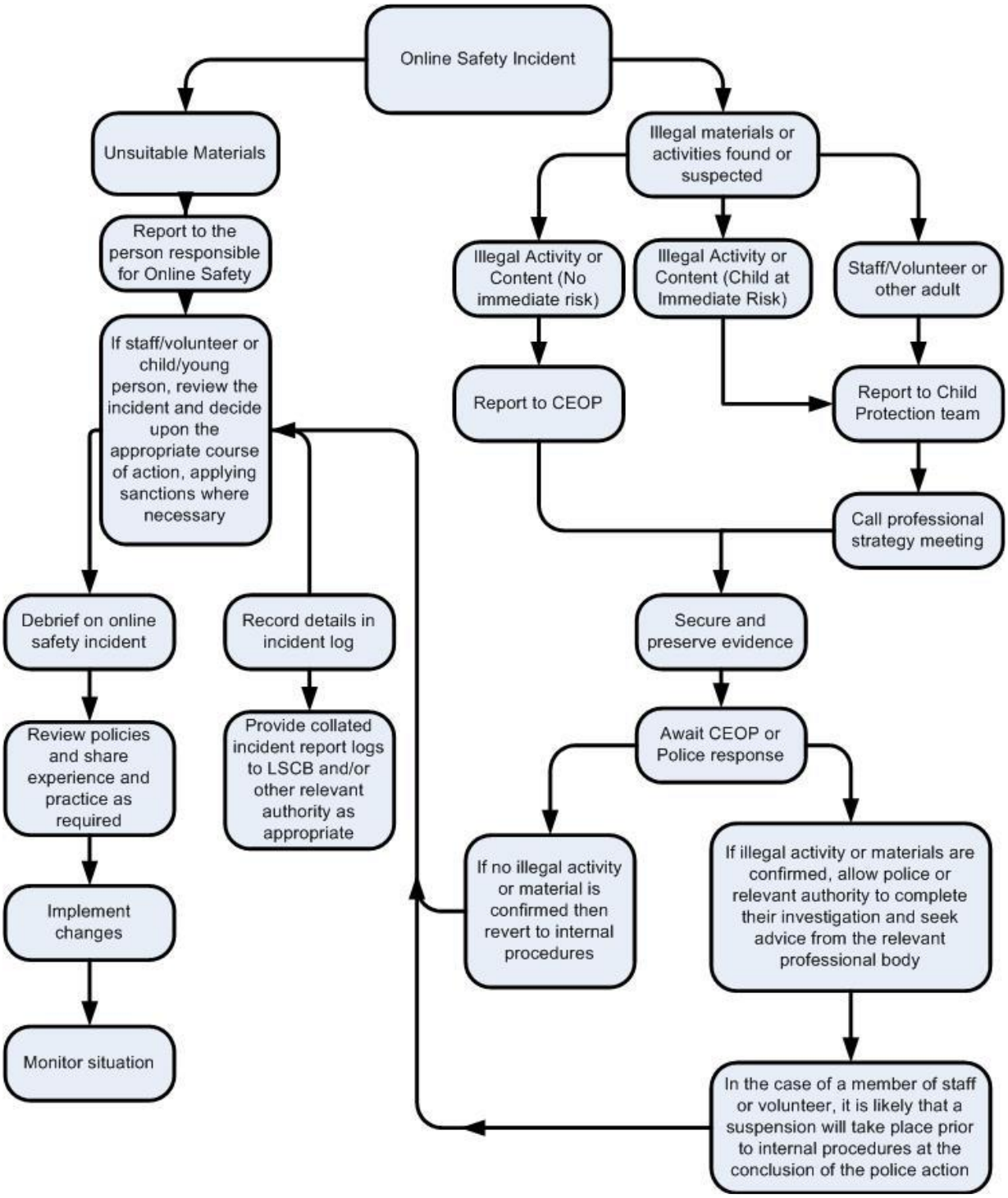
Work devices must be used solely for work activities.

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 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 disciplinary procedures/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.



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).

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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. All incidents and follow up actions are recorded on CPOMs.

This policy will be reviewed every 2 years by the ICT co-ordinator. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1:

St Cuthbert's C of E Primary School

The Chase, Great Glen, Leicester LE8 9EQ Tel: 0116 2592764

KS1 Acceptable Use Policy

ICT is used in school to enhance our learning:

- I will only use ICT equipment if a teacher has asked me to
- I will not tell my password with my friends
- I will not share my name, age , where I live, my family or pets
- I will only click on pages that my teacher has asked me to
- I will not take photos of others unless I have asked
- If I see anything that makes me sad, I will tell a teacher straight away
- I will show my teacher if I get a message
- I will look after the ipad or laptop that I am using and tell my teacher if it is not working
- I will make sure that I have turned off my laptop/ipad when I have finished with it

Anything that I do on a computer may be seen by someone else!

Child's name	Signature	Date

Appendix 2:

St Cuthbert's C of E Primary School

The Chase, Great Glen, Leicester LE8 9EQ Tel: 0116 2592764

KS2 Acceptable use policy

ICT in school is used to enhance the children's learning

When I use school ICT equipment, I promise I will:

- Only use school computer or ICT equipment when a teacher is present
- Keep my username and password safe and not share it with anyone
- Not share my personal information (name, age, where I live, my family)
- Tell an adult if something makes me feel uncomfortable
- Always log off and shut my computer or piece of ICT equipment when I have finished using it

I will not:

- Go on any website without my teacher's permission
- Log on using another pupil's login
- Click on any links unless I have permission
- Arrange to meet anyone online
- Use any language that is not appropriate
- Use any personal devices in school

I understand that the school will monitor any website that I go on and there will be consequences if I do not follow the rules.

ICT Acceptable Use policy

Child's name	Signature	Date

Appendix 3:

Acceptable User Policy (Parent)

Parent Acceptable Use Agreement

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the internet at the school;
- the school's chosen email system;
- the school's online learning environments;
- ICT facilities and equipment at the school.

- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
- I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video:

- I understand the school has a clear policy on "The use of digital images and video" (see below) and I support this.
- I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.
- I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.
- I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites:

I understand that the school has a clear policy on "The use of social networking and media sites" (see below) and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____ **Date:** ___/___/___

The use of digital images and video (Parents)
To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

- **If the pupil is named, we avoid using their photograph.**
- **If their photograph is used, we avoid using the pupils' full name.**

Where showcasing examples of pupils work we only use their first names, rather than their full names.
If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
Only images of pupils in suitable dress are used.
Staff taking photos for school purposes must only do so using school equipment, but where such equipment is not available then personal devices can be used. In using a personal device, staff will ensure that:

- photos or videos are not uploaded to their personal cloud-based storage;
- photos or videos are, at the earliest opportunities forwarded to the Headteacher and then deleted from personal devices;
- photos and videos will not to be forwarded to unsecure email addresses

Examples of how digital photography and video may be used at the school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity; e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint© presentations.

- You child's image being used on school Social Media accounts and websites.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, school or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our academy prospectus.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media
This school asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

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?	
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?	
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?	