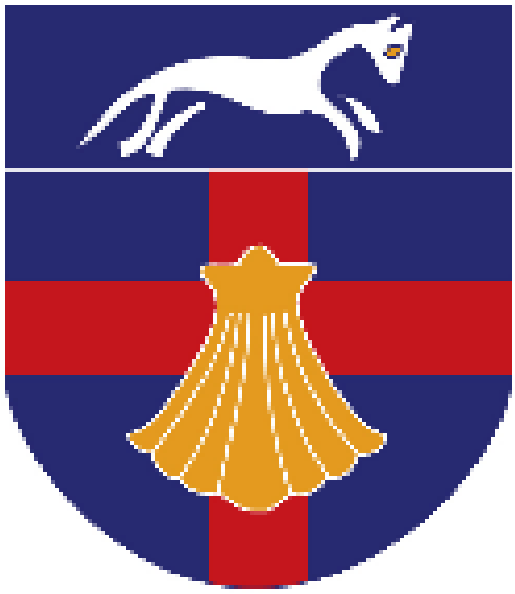
January 2019

Review due: January 2021

Radley CE Primary School

Online Safety Policy



Contents

1. Aims

Our school aims to:
Have robust processes to ensure the online safety of children, 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 statutory safeguarding guidance, Keeping Children Safe in Education Sept 2018, and its advice for schools on preventing and tackling bullying and 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

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

The **headteacher** – **Grace Slater** - has a duty of care for ensuring the safety (including e-safety) of members of the school community. The headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. In her role as Designated Safeguarding Lead (DSL), the headteacher is trained in e-safety issues and aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers; potential / actual grooming incidents
- cyber-bullying

It is the responsibility of the headteacher to confirm that the technical support service provider (Koala IT) carries out measures, which ensure that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets required e-safety technical requirements and any Local Authority online safety policies and guidance that may apply.

The **IT Subject Leader** – Anne Quigley

- takes day-to-day responsibility for e-safety issues.
- has a leading role in establishing and reviewing the school e-safety documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- liaises with the technical support service provider: Koala IT.

Teaching and support staff are responsible for ensuring that they
- have an up to date awareness of e-safety and of current school e-safety policy / practices.
- have read, understood and agreed to the Acceptable Usage Policy for Staff.
- report any suspected misuse or problem to the headteacher.
- Ensure pupils understand and follow the Acceptable Usage Policy for Pupils

Pupils are responsible for using the school digital technology systems in accordance with the Acceptable Usage Policy for Pupils.

3.1 The Governing Body

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

The governing board will ensure there are regular meetings with appropriate staff to discuss online safety, and monitor any online safety logs as provided by the designated safeguarding lead (DSL). The link governor overseeing online safety is Sue Sowden – the school's Safeguarding Governor

Governors will ensure they have read and understand this policy, agree and adhere to the terms on acceptable use of the school's IT systems and the internet (Appendix 2)

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) – Grace Slater; and Deputy Safeguarding Lead - Julie Ilsley, are set out in our Child Protection Policy.

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

In ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the technical support service provider (Koala IT – Stuart Wicker) and IT Subject Lead – Anne Quigley, as necessary, to address any online safety issues or incidents

Ensuring that any online safety incidents are logged (see Appendix 4) 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 ensuring delivery of staff training on online safety (Appendix 3 self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Ensuring the provision of regular reports on online safety in school to the governing board

3.4 The Technical Support Service Provider (Koala IT)

The technical support service provider (Koala IT) 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 IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Conducting full security checks and monitoring the school's IT systems on a regular basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.5 The IT Staff Lead

The IT Lead is responsible for:

Ensuring that any online safety incidents, including any incidents of cyber-bullying, are logged (see Appendix 4) and dealt with appropriately in line with this policy

3.6 All Staff and volunteers

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

Maintaining an understanding of this policy, and implementing it consistently.

Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (Appendix 2), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1)

Working with the DSL to ensure that any online safety incidents are logged (see Appendix 4) 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

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 IT systems and internet (Appendix 1)

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

What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.8 Visitors and members of the community

Visitors and members of the community who use the school's IT 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 2).

4. Educating pupils about online safety

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

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

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.

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.

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 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 to 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

The school also sends information 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 children, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (Appendices 1 and 2). 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 and 2.

8. Pupils using mobile devices in school

Children may not bring mobile devices into school. Should they do so, these will be held in the office until the end of the day, and parents informed.

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 2.

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. 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 technical support service provider (Koala IT).

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. 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 IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents 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 Deputy DSL 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 and volunteers will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. More information about safeguarding training is set out in our Child Protection policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues, related to online safety. An incident report log can be found in Appendix 4.

This policy will be reviewed by the Curriculum Committee on a two yearly basis.

13. Links with other policies

This Online Safety policy is linked to our:

Child Protection policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

January 2019

Review due: January 2021

Appendix 1: Acceptable Use Agreement (Children and Parents / Carers)

Acceptable Usage Policy for Pupils

You should follow these guidelines whenever you are using the internet (for work or fun activities and games) in and out of school.

Be **SMART** online at Radley CE Primary School!

- **S**afe: Keep your personal information safe. Think carefully before sharing information or pictures.
- **M**eeting: Never arrange to meet an online friend because it can be dangerous.
- **A**ccepting: Do not accept emails, messages and friend requests from people that you don't know. If you receive a message that makes you feel uncomfortable, don't reply! Instead, tell an adult that you trust.
- **R**eliable: Information on the internet may not be true. Not everyone online is who they say they are.
- **T**ell: If you feel uncomfortable or worried, tell an adult that you trust.

Online Safety Acceptable Usage Policy for Pupils

Child

My parents and I have read the Online Safety Acceptable Usage Policy and I agree to follow it.

Child's signature: _____

Parents / Carers

As a parent or carer, I have read, discussed and explained the Online Safety Acceptable Usage Policy with my child. I understand that if he/ she fails to follow the Online Safety Acceptable Usage Policy, his/her internet access may be withdrawn and I will be informed.

Parent / Carer's signature: _____ Date: _____

Copyright Release

The school may include children's work on web pages, ICT presentations, educational or interest articles for magazines or similar. Please rest assured the child's safety will always be of paramount importance and no personal information will be made public. Please sign this copyright release if you are happy for your child's work to be shared in this way. (This can be changed at any time: please see the Headteacher or IT Co-ordinator).

I consent for the school to publish my child's work on the internet, subject to strict confidentiality of personal information.

Parent / Carer's signature: _____

Appendix 2: acceptable use agreement (Staff)

Acceptable Usage Policy for Staff

Acceptable use of the school's IT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name:	
When using the school's IT systems and accessing the internet, I will not: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature 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 Share my password with others or log in to the school's network using someone else's details	
I will only use the school's IT systems and access the internet 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. 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 IT Co-ordinator know if a child 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 deal with incidents of cyberbullying in accordance with the school's behaviour and anti-bullying policies. I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed:	**Date:**

Appendix 3: Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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? Please record them here.	

Appendix 4: Online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 5: Ten top tips for children and parents

The Children's Commissioner's Office Report 'Who Knows What About Me?' Nov 2018 has brought the keysteps together below:

Ten Top Tips for Parents and Children

For children

1. Stop and think when you're about to share some personal information. Ask yourself, "Do I need to share this"? If you can't do what you want (e.g. play a game) without giving away this information, ask yourself, "Is it worth it?" – sometimes it is, but lots of times it isn't.

2. Read our Digital 5 A Day guide if you spend lots of time online and on social media, to help you think about other ways you can spend your time: connect, be active, get creative, give to others and be mindful.

3. Look through terms and conditions to understand what data is collected when you use social media, websites and gadgets. We've simplified some here.

4. Mute smart speakers when you don't want them to listen to you.

5. Talk to an adult you trust if you are worried about someone else knowing something about you, or if you want to learn more about your data rights.

For parents/carers

1. Don't post photos and videos which reveal personal information about your children online. Sometimes it isn't obvious – for example, tagging a child at home on their birthday gives away their date of birth and home address.

2. Change the default passwords on all the gadgets your children use – whether it's a smart speaker, internet - connected toy or location - tracking watch. Don't forget the router!

3. Make sure the gadgets you buy your children are genuine. Counterfeit versions can be less secure than the originals.

4. Watch out for security updates and install them as soon as you are prompted.

5. Talk to organisations that hold information about your child about what information they collect and why, including schools, online services and retail loyalty schemes. Raise any concerns you have.