



Belgrave Road
Uppingham
Rutland
LE15 9RT

01572 823245
uppinghamoffice@rltschools.com
www.uppinghamprimary.co.uk

Headteacher: Mrs J Exton

Online Safety Policy

February 2020

This policy was reviewed by the IT lead and approved by
Governors in March 2020.

Signed (Headteacher)

Date.....

Signed (Governor)

Date.....

Date of review:

Online Safety Policy

Our online safety Policy has been written by the school, drawing on current government guidance and takes into account the National Curriculum Computing Programmes of Study. It has been agreed by senior management and approved by the governors. The online safety Policy and its implementation will be reviewed annually.

Definition

Online safety refers to the use of electronic and mobile devices that children, young people and adults may have access to. It is about ensuring each individual is equipped with the knowledge and understanding of the risks involved when accessing online content to enable them to protect their personal information as well as their wellbeing and safety.

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

Roles and Responsibilities

The governing board

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

All governors will:

- Ensure that they have read and understand this policy

The headteacher

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

The designated safeguarding lead

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

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 incidents of online safety or cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary

The ICT manager (ARK)

The ICT manager 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 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 and dealt with appropriately in line with this policy and behavior policy.

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 (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>
- National Online Safety Website <https://nationalonlinesafety.com/>

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 2).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum following the DFE Education for a Connected World <https://www.gov.uk/government/publications/education-for-a-connected-world> focusing on the following aspects of online information.

- Self image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

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 also use assemblies and a dedicated online safety day/week to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Where possible, online safety rules will be displayed where computers are used and discussed with the pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

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. Online safety will also be covered during open afternoon sessions, throughout the year.

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.

Cyber-bullying

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.

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 pupils, and the issue will also be addressed in assemblies.

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.

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.

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 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.

Email

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Pupils may only use approved e-mail accounts for school purposes.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. Access in school to external personal email accounts may be blocked.

Staff should not use personal email accounts for professional purposes.

Published content including the school website and Class Dojo.

The school is keen to celebrate pupils' work and promote the school.

The point of contact on the website is the school address, school e-mail and telephone number. Staff or pupils' personal information is not published.

The headteacher and Office Manager will take overall editorial responsibility of the website and ensure that content is accurate and appropriate.

The school website will comply with the school's guidelines for publications, including respect for intellectual property rights, privacy policies and copyright.

Publishing pupil's images and work

Images or videos that include pupils will be selected carefully based on permissions given from parents.

These images will also ensure that all children, including those with particular or distinct disabilities, are sympathetically composed to show them at their best.

Pupils' full names are not used anywhere on the website or other online space such as Class Dojo or Facebook, particularly in association with photographs.

Written permission from parents or carers is obtained before photographs of pupils are electronically published.

Work can only be published with the permission of the parents/carers.

The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.

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. Staff are not permitted to use an electronic device such as a USB to save data protected work. All work should be saved directly onto the hard drive of the password protected work device in line with GDPR guidance.

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

Work devices must be used solely for work activities.

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 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 ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

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 and staff meetings).

The 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 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.

Monitoring arrangements

Every member of staff is expected to log behaviour and safeguarding issues related to online safety as well as reporting this information to the DSL.

This policy will be reviewed yearly by the Computing Subject Lead. At every review, the policy will be shared with the governing board.

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
- Complaints procedure

Date reviewed: February 2021

Appendix 1: 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:

When using the school's ICT systems and accessing the internet in school, I will not:

Use them for a non-educational purpose

Use them without a teacher being present, or without a teacher's permission

Access any inappropriate websites

Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)

Use chat rooms

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

Share my password with others or log in to the school's network using someone else's details

Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer

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.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):

Date:

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 for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the 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, 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 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.

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: