Forest Academy & Elveden Church of England Primary Academy

Online Safety Policy, mobile devices & acceptable use

Date Completed – December 2017

Completed by Kathy Harris

Agreed by Headteachers

Signed on behalf of Governors _____

Review December 2018

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 appropriate2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, 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

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 body 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).

The governor who oversees online safety is Helen Morley

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

3.2 The Headteachers

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

3.3 The designated safeguarding lead and alternate designated lead

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

The ADL has additional Online Lead Training and 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 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 staff training on online safety is delivered
- 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 and ADL work together to ensure the online safety of children, staff and school systems.

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
- Conducting a full security check and monitoring the school's ICT systems on a termly basis (when the school is closed).
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive and will be implemented by the ICT Technician

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 and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged 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

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

3.7 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

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 or Facebook page. This policy will also be shared with parents.

Online safety will also be covered during sessions run for parents/carers and through notifications e.g. through Facebook, to allow us to respond to and prevent potential issues as they occur.

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/ADL.

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.

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. Teachers will discuss cyber-bullying with their classes, and the issue will 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.

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).

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/ADL 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. 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.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but these must be left at the front office throughout the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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.

8.1 Staff using mobile devices in school

Staff should not use their mobile phones during their working hours (this does not include break and lunch times) and phones should be kept in bags out of sight when working with children. Staff are asked to keep their contact details up to date with the School Office.

8.2 Parents using mobile devices in school

Parents are asked not to use mobile phones once they are inside the school, this includes the Reception area. Camera phones are not to be used during school assemblies and other open events due to Safeguarding reasons.

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.

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.

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 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.

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 alternates 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/ADP logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the Headteachers. At every review, the policy will be shared with the governing body.

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

Forest Academy
Bury Road, Brandon
Suffolk, IP27 0FP
Tel: 01842 810309
E mail: forestadmin@forestacademy.co.uk
Headteachers: Mrs A Grimes and Mrs L Rourke

Staff and Governor
Acceptable Use Agreement / Code of Conduct

The school Acceptable Use Policy is designed to ensure that all staff are aware of their responsibilities when using any form of Information & Communications Technology within their professional role. All staff are expected to sign this policy and adhere at all times to its contents.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.
- I will not discuss school issues on social networking sites / web-blogs.
- I will not give out to pupils, my own personal contact details, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) and VLE tools for communications related to my professional role.
- I am aware that communicating with parents of students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter.
- I will **not** communicate with any pupil via private email / SMS and social networking sites and will notify the senior designated person if a child contacts me.
- I will check my security settings every month and activate the Review Posts setting so that my personal information is kept securely.
- I will not refer to Forest Academy or Elveden Academy in any capacity on social networking sites.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that I only take school personal data off school site in encrypted form, or will access the data remotely.
- I will not install any hardware or software without permission of the ICT leader
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. **I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.**
- Images & videos of pupils and / or staff will only be taken, stored on school equipment and will only be used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images & video will not be distributed outside the school network / VLE without the permission of the parent/ carer, member of staff or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ..... Date .....

Full Name .....(printed)

Job title .....

Company Number: 07400940
Working in Partnership with
Elveden Church of England Primary Academy.

Elveden Church of England Primary Academy
London Road, Elveden
Suffolk, IP24 3TN
Tel: 01842 890258
E mail: office@elvedenacademy.co.uk
Headteachers : Mrs L Rourke and Mrs A Grimes

1st March 2017

Dear Parent/ Carer

ICT including the Internet, email and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school.

Yours faithfully

Mrs Rourke and Mrs Grimes

Acceptable Use Agreement

We have discussed this and .....(child name) agrees to follow the Online Safety rules and to support the safe use of ICT at Elveden C of E Primary Academy.

Parent/Carer Signature ..... Class .....

Date .....

Company Number: 08327233
Working in Partnership with
Forest Academy

Forest Academy
Bury Road, Brandon
Suffolk, IP27 0FP
Tel: 01842 810309
E mail: forestadmin@forestacademy.co.uk
Headteachers: Mrs A Grimes and Mrs L Rourke

1st March 2017

Dear Parent/ Carer

ICT including the Internet, email and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school.

Yours faithfully

Mrs Grimes and Mrs Rourke

✂---

Acceptable Use Agreement

We have discussed this and ………………………………………(child name) agrees to follow the Online Safety rules and to support the safe use of ICT at Forest Academy.

Parent/Carer Signature ……………………………………………………

Class ………………………………… Date ………………………………

Company Number: 07400940
Working in Partnership with
Elveden Church of England Primary Academy.

Online Incident Report Form

Date of incident:	Time of incident: (if known)
Pupil Name:	
Location of incident:	
Information received from: (pupil/parent/staff/other)	
Brief Description of Incident:	
Comments/Notes/Actions	

Signature of reporting person_____Date: _____

Signed by Online Safety Coordinator _____Date:_____