

***Online Safety Policy, mobile devices***

***& acceptable use***

Date Reviewed – September 2024

Completed by Anna Syer

Agreed by Headteachers

Signed on behalf of Trustees\_\_\_L.Proudlock\_\_\_

Review September 2027

# 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 to Legislation and guidance

2. Policy support

This policy is based on the Department for Education’s statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on [preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation) and teaching [online safety](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)  It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), 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](https://www.gov.uk/government/publications/national-curriculum-in-england-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 safetyand monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Paul Tams as referenced in ‘**Recommendations on Committee Structure and Terms of Reference’ – Elveden Academy web site**

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 lead 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 and have the ability to use, SYPE, Teams and Zoom when needed
* 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 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.
* Filtering and monitoring is provided by Surf protect - as discussed with Mark – ICT support
* 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. These are shared with governors termly.
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy. These are shared with governors termly.

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

**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 (appendix B)

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>
* Wake up Wednesday : <https://nationalonlinesafety.com/>

**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 and parent mail messages. 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/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 and police are made aware.

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](https://www.gov.uk/government/publications/searching-screening-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 (appendix A). 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 using Surf protect Monitor Managed Service the websites and online platforms 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 in the school office’s locked desk draw or cupboard. .

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

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 lead.

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. The incident will be logged on an online report form (appendix c) and CPOMS.

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 ( prevent).

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, hot topics).

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 as 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 is supported at Elveden by **Smoothwall Monitor Managed Service**

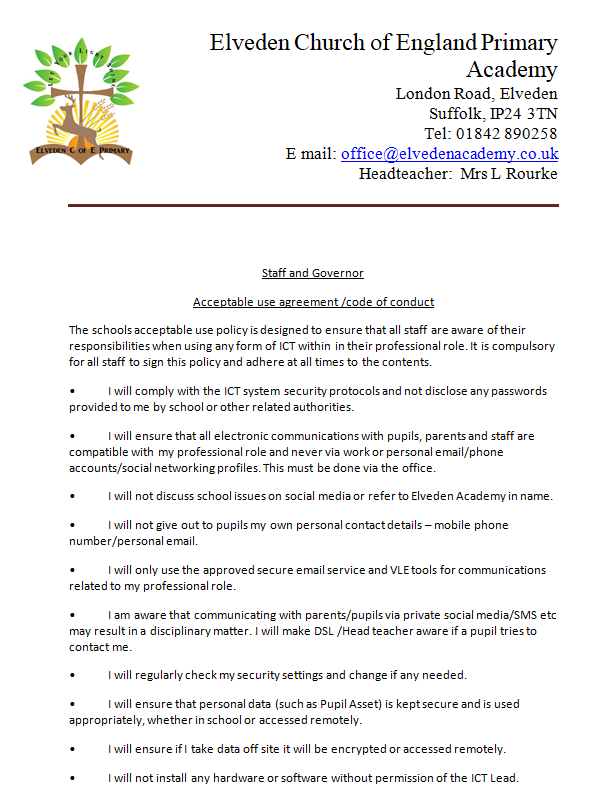
This policy will be reviewed annually by the Headteachers. At every review, the policy will be shared with the governing body.

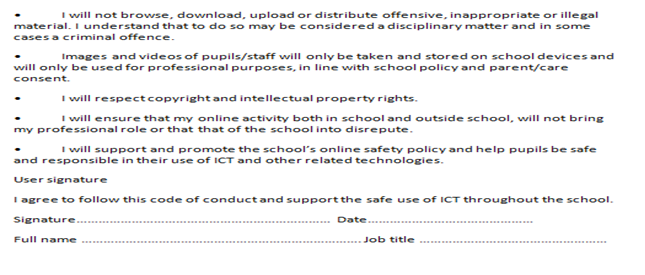
# 13. Links with other policies

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
* Tapestry Scheme (appendix d)

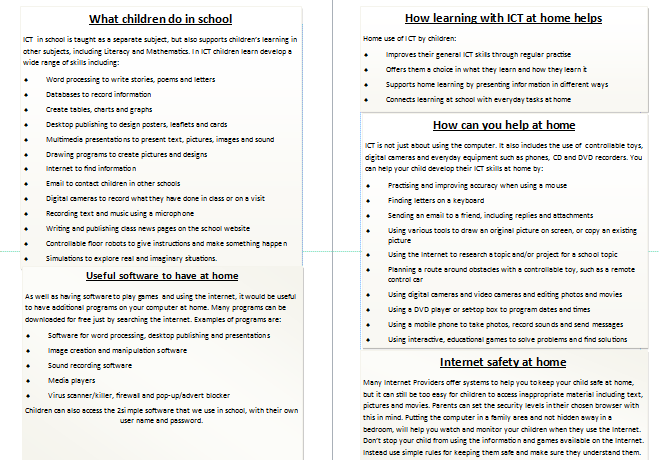
Appendix A

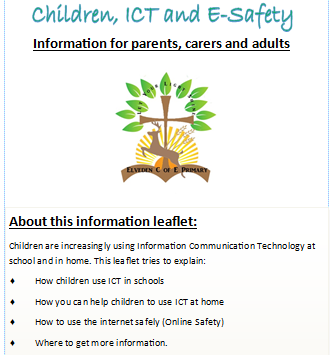


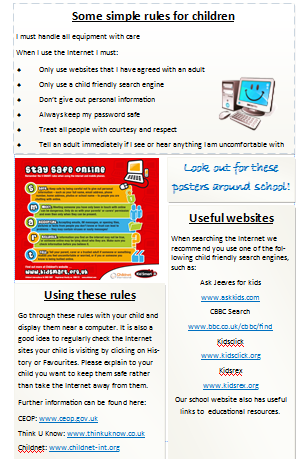


Appendix B

# 









Appendix C

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:\_\_\_\_\_\_\_\_\_\_\_\_

Appendix D

Elveden Church of England Primary

Academy

Tapestry Scheme

(This scheme should be read in conjunction with our online policy)

Date Completed: September 2024

Completed by: Anna Syer

Review Date: September 2027

Elveden

Tapestry Policy

Purpose

Tapestry is an online assessment tool where staff can add assessments and “wow” moments from the children’s learning to go into their individual e-profile. Parents can access their own child’s assessments and add observations about achievements children have made at home.

Aims

* To protect all information, staff, children and parents following e-safety rules.
* To make sure only the appropriate adults can access the assessments and photos.
* To make sure the correct information and photos are uploaded

Guidance

* Only the individual child will be named in their own assessment. Other children will be called friend/child.
* The class teacher and teaching assistants have to check observations before they are sent to the e-profile.
* Photos must include the child who the assessment is for and may contain other children.
* Children can be in other children’s photos unless a parent requests for them not to be
* Observations should celebrate achievements
* Descriptions may be brief but must be precise and relevant
* We will regularly delete the photos from the iPad after posting on tapestry
* All information will remain on i-cloud and will only be accessible using the correct passwords. No information is stored on any iPad or devices.
* Usernames and passwords must not be given to any other member of staff or volunteer. Supply staff must be logged on by another member of staff.