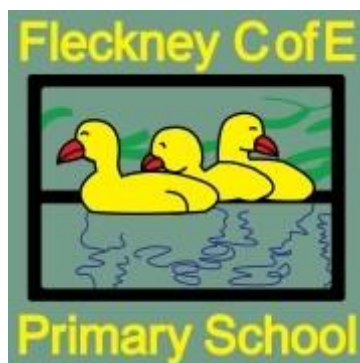


# **Fleckney C of E Primary School**

## **E-Safety Policy**



**‘Let your light shine’**

**Matthew 5:16**

**Be the best that you can be !**

### **Our Vision**

**Fleckney Church of England Primary School is a place where kindness, compassion and respect are at the heart of everything we do. We aspire for everyone to thrive and flourish and achieve our full potential in every aspect of school life. Through our Christian values, we nurture self-confidence, resilience and a sense of community so that we have an understanding of ourselves and our place in the wider world.**

**Date of Policy: October 2024**

**Drafted by: J.Richards**

**Approved by: J.Richards and G.Robinson**

**Date of Review: October 2026**

## Table of Contents

1.	<u>Aims</u>	4
2.	<u>Legislation and guidance</u>	4
3.	<u>Roles and responsibilities</u>	4
4.	<u>Educating pupils about online safety</u>	7
5.	<u>Educating parents about online safety</u>	8
6.	<u>Cyber-bullying</u>	8
7.	<u>Acceptable use of the internet in school</u>	9
8.	<u>Pupils using mobile devices in school</u>	9
9.	<u>Staff using work devices outside school</u>	9
10.	<u>Staff use of personal devices</u>	10
11.	<u>Email and Social Networking</u>	10
12.	<u>Copyright</u>	11
13.	<u>How the school will respond to issues of misuse</u>	11
14.	<u>Training</u>	11
15.	<u>Monitoring arrangements</u>	12
16.	<u>Links with other policies</u>	12
17.	<u>E-safety Incident (not concerning children) e.g. pop-ups</u>	12
	<u>Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)</u>	<u>13</u>
	<u>Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)</u>	<u>14</u>
	<u>Appendix 3: Online Safety Training Needs – Self-Audit For Staff</u>	<u>15</u>
	<u>Appendix 4: : E-Safety Incident reporting form (not concerning children)</u>	<u>16</u>

# Fleckney C.E. Academy

## E-Safety Policy

### 1. Aims

1.1. Fleckney C of E Primary Academy 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, reporting any incidents on CPOMS using the 'Online/E-Safety tag'.

### 2. Legislation and guidance

- 2.1. 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](#).
- 2.2. 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.
- 2.3. This policy complies with the Fleckney C of E Primary Academy funding agreement and articles of association.

### 3. Roles and responsibilities

#### The Fleckney C of E Primary Academy Governors

- 3.1. The Fleckney C of E Primary Academy Governors approve this policy and delegates responsibility for its implementation at school level.

#### Governing Bodies (GB)

- 3.2. The GBs have responsibility for monitoring this policy and holding headteachers to account for its implementation.
- 3.3. The GB will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs (CPOMS) as provided by the school's designated safeguarding lead (DSL).
- 3.4. Each school will appoint a Governor who oversees safeguarding, including online safety.

3.5. All local governors will:

- Ensure that 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 and the Fleckney C of E Primary Academy Data Protection Policy.

#### **The headteacher**

3.6. 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**

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

3.8. 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, ICTIC, Computing Lead, School Office Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (on CPOMS) 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 3 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
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.9. This list is not intended to be exhaustive.

#### **The ICT Management Form (ICTIC), Computing Lead and School Office Manager**

3.10. ICTIC, Computing Lead and School Office Manager are responsible for:

- Putting in place appropriate filtering and monitoring systems (SENSO), 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 a full security check and monitoring the school's IT systems on a half termly 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 (CPOMS) and dealt with appropriately in line with this policy

3.11. This list is not intended to be exhaustive.

## All staff and volunteers

- 3.12. 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 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 (CPOMS) and dealt with appropriately in line with this policy
  - Ensure children in their classes have read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendix 1)
  - The agreement should be completed year as a class. Teachers will go through the acceptable use agreement (appendix 1) in their first computing lesson, ask the children to sign it. Ensuring that children understand the school expectations.
- 3.13. This list is not intended to be exhaustive.

## Parents

- 3.14. Parents are expected to:
- Notify a member of staff, office staff ([admin@Fleckney.leics.sch.uk](mailto:admin@Fleckney.leics.sch.uk)) or the headteacher of any concerns or queries regarding this policy (concerns should then be logged on CPOMS)
- 3.15. 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>
  - NSPCC online safety advice: <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>
  - Net Aware NSPCC and O2: <https://www.net-aware.org.uk/>
  - 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>

## Visitors and members of the community

- 3.16. 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, (e.g. if they are planning on using the school's internet) they will be expected to agree to the terms on acceptable use (appendix 2).

## 4. Educating pupils about online safety

- 4.1. Pupils will be taught about online safety as part of the curriculum.
- 4.2. 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
- 4.3. 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
  - How to report a range of concerns
- 4.4. The safe use of social media and the internet will also be covered in other subjects where relevant.
- 4.5. 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.
- 4.6. The following links are from Keeping Children Safe in Education and may be used within school:
  - DfE advice for schools: teaching online safety in schools  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/811796/Teaching\\_online\\_safety\\_in\\_school.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf)
  - UK Council for Internet Safety (UKCIS)27 guidance:  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/896323/UKCIS\\_Education\\_for\\_a\\_Connected\\_World\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf)
  - National Crime Agency's CEOP education programme: <https://www.thinkuknow.co.uk/>
  - Public Health England: <https://campaignresources.phe.gov.uk/schools/topics/mental-wellbeing/overview> Rise Above

## 5. Educating parents about online safety

- 5.1. Fleckney C of E Primary Academy 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 via our school website.
- 5.2. Online safety will also be covered within parent communication via our school website.
- 5.3. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Key Stage Leader, headteacher and/or the DSL.
- 5.4. Concerns or queries about this policy can be raised with any member of office staff, staff or the headteacher.

## 6. Cyber-bullying

### Definition

- 6.1. 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's Positive Behaviour and Discipline Policy including Anti Bullying Guidance)

### Preventing and addressing cyber-bullying

- 6.2. 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.
- 6.3. 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.
- 6.4. 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 (PSHCE) education, and other subjects where appropriate.
- 6.5. 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).
- 6.6. Fleckney C of E Primary Academy will also send information on cyber-bullying to parents (Via our School Website) so that they are aware of the signs, how to report it and how they can support children who may be affected.
- 6.7. 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.
- 6.8. 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.

### Examining electronic devices

- 6.9. The DSL has 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, this should be reported on CPOMS.

- 6.10. 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:
- 6.11. 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
- 6.12. Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).
- 6.13. 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

- 7.1. All pupils, 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 (for example, if they are intending to use the school's internet).
- 7.2. 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.
- 7.3. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- 7.4. More information is set out in the acceptable use agreements in appendices 1 and 2.

## 8. Pupils using mobile devices in school

- 8.1. Year 5 and 6 Pupils (Year 4, in exceptional circumstances) may bring mobile devices into school, but are not permitted to use them during the school day. Pupils who need mobile phones to communicate with their parents or carers for safety reasons on the way to and from school may leave their phones securely at the school office during the school day and collect them at home-time. They will remain off from 8:30 – 3:15 or until the child is offsite.

## 9. Staff using work devices outside school

- 9.1. Staff members using a work device outside school for work or personal use 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.
- 9.2. Staff may use work devices for reasonable personal use out of school hours (e.g. using the internet in line with this policy or checking personal email accounts). Email attachments must not be opened



on a work device unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- 9.3. Personal files (e.g. photographs, music, documents) and passwords must not be stored on a work device. Staff are reminded that all files saved on their work device are synced with the server and that their work device may need to be handed in without prior notice for checking, repairs or updates.
- 9.4. School devices must not be used to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (e.g. child sexual abuse images, criminally racist material, adult pornography, material which incites hatred or discrimination, material which promotes gambling or any form of online risk-taking, material which is degrading to any individual or group).
- 9.5. Staff must ensure that their work device is secure, encrypted 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.
- 9.6. If staff have any concerns over the security of their device, they must seek advice from ICTIC, the Computing Lead, headteacher and/or School Office Manager

## **10. Staff use of personal devices**

- 10.1. Staff members must not use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- 10.2. All staff, volunteers and students must ensure that their mobile phones, personal cameras and recording devices are not used for personal use in school and are stored securely during working hours in teaching areas and any other area of the school where children are present. Mobile phones must not be used for making personal phone calls, texting, or accessing personal social media sites in any teaching area in school during lesson times or whilst children are present.
- 10.3. All telephone contact with parents or carers must be made using the school landline or mobile phone, or on the rare occasion where a personal phone is needed, staff must withhold their number.
- 10.4. Where possible, all school related work should be carried out on a work device. In the case where a personal computer or laptops is used, staff must ensure that no personal data or sensitive data is stored on that device.

## **11. Email and Social Networking**

- 11.1. Staff members and governors must use the email address provided by the school for all school-related communication.
- 11.2. School devices may not be used to access social networking sites for personal purposes on the school site but may be used to access and update the school's own social networking accounts.
- 11.3. Staff, students and volunteers are reminded that social networking sites should be regarded as public forums and as such any discussion about school issues, colleagues or pupils is strongly discouraged. Any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school will result in disciplinary action.
- 11.4. Staff members must make every effort to ensure that neither their personal/professional reputation, or the school's reputation is compromised by inappropriate postings on social media and must not

disclose any confidential or sensitive information, or information or images that might compromise the security of the school.

- 11.5. Staff members must not share personal information with a pupil (e.g. personal phone number or email address) or communicate with pupils via personal social networking accounts.

## **12. Copyright**

- 12.1. Staff must ensure that they have permission to use the original work of others in their own or their pupils' work. Where work is protected by copyright (including music and videos), it must not be copied, downloaded or distributed without permission from the copyright holder.

## **13. How the school will respond to issues of misuse**

- 13.1. 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.
- 13.2. 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.
- 13.3. Incidents which involve illegal activity or content will be reported to the police.

## **14. Training**

- 14.1. All new staff members will receive training from the headteacher, deputy head teachers, phase leaders and/or school office manager, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- 14.2. All staff members will receive refresher regularly year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- 14.3. 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.
- 14.4. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- 14.5. Volunteers will receive appropriate training and updates, if applicable.
- 14.6. More information about safeguarding training is set out in our child protection and safeguarding policy.

## **15. Monitoring arrangements**

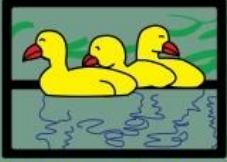
- 15.1. The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.
- 15.2. This policy will be reviewed bi-annually at the latest by the headteacher, ICTIT, the Computing Lead, School Office Manager and DSLs. At every review, the policy will be approved by the Governors.

## **16. Links with other policies**

- 16.1. This online safety policy is linked to our:
- Child protection policy
  - Behaviour policy
  - Anti-bullying policy
  - Staff Code of conduct
  - Data protection policy and privacy notices
  - Complaints procedure

## **17. E-safety Incident (not concerning children) e.g. pop-ups**

- 17.1. Where an E-Safety incident occurs that does not involve or compromise any children, for example a pop-up from a website, staff, visitors or governors should fill out the form attached (appendix 4) and report the incident a DSL.



## Appendix 1: Acceptable Use Agreement (Pupils)

The agreement should be completed year as a class. Teachers will go through the acceptable use agreement (appendix 1) in the first computing lesson of the year (where applicable), ask the children to sign it. Ensuring that children understand the school expectations.

### Acceptable use of the school's IT systems and internet: agreement for pupils

**Class:**

When using the school's computers or i-Pads and using the internet in school, we will not:

- Use them for anything other than for learning
- Use them when a teacher is not there, or without a teacher's permission
- Access any websites other than the sites the teacher has told us to use
- Access sites such as Facebook, Twitter or any other social media.
- Use chat rooms or any platform in which we can chat to others online (this is where you can talk to other people on the computer)
- Open any anything in emails, or follow any links that you can click on in emails, without first checking with a teacher
- Type any inappropriate language on the computer
- Share my password with others or use anyone else's computers details like their user name or password
- Give my information about me like my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Arrange on the computer to meet anyone in person/ at the park/ outside of school without first consulting my parent/carer, or without adult supervision

Year 5 and 6 Pupils: If we bring a personal mobile phone or other personal electronic device into school, we will turn it off, hand it to the office, collect it at the end of the day and not turn it on until out of the school gates.

We agree that the school will know the websites we visit.

We will immediately let a teacher or anyone that works at the school know if we see anything on the computer that upsets, distresses or might harm us or others.

We will always use the school's computer and internet responsibly.

**Signed (by teacher on behalf of pupils):**

**Date:**

**Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)**

**Acceptable use of the school's IT systems and the internet: agreement for staff, governors, volunteers and visitors**

**Name of staff member/governor/volunteer/visitor:**

I have read and agree to abide by the school's E-Safety Policy.

I will only use the school's IT 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 or for reasonable personal use in-line with this policy.

I agree that the school may 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 ICTIC 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 IT systems and internet responsibly, and ensure that pupils in my care do so too.

**Signed (staff member/governor/volunteer/visitor):**

**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 IT 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.

# E-Safety Incident Reporting Form (non-student)

Date	Time	Staff Name
<b>Location / Device</b>		

<b>Incident/Concern</b>

<b>Action</b>

<b>Reported by:</b>	<b>Role:</b>

