



E-Safety Policy
Policy Number
Date of Issue: February 2021
Review Date: Annually

Fellside Community Primary School

Ensuring every member of our school community is inspired to fulfil their potential and is prepared effectively for their future.

Fellside Community Primary School

E-Safety Policy Statement 2021-2024

Rationale:

The potential that technology has to impact on the lives of all people increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than adults. In many areas, technology is transforming both the way schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. These trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use, which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we help those who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and Leadership

All at Fellside Community Primary are committed to safeguarding children in our care. This policy has been developed by the e-safety/computing co-ordinator and the Senior Leadership Team in order to ensure that it truly reflects our robust and thorough approach to safeguarding. This section outlines responsibilities of staff, leaders and stakeholders as well as all users of technology within school.

Responsibilities of the E-Safety / Computing Co-ordinator

Our e-safety co-ordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety co-ordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
- Provides training and advice for staff.
- Liaises with the Local Authority where necessary.

- Liaises with school IT technical support to ensure that internet access is appropriately filtered.
- Receives reports of e-safety incidents and maintains a log of incidents to inform future e-safety developments.
- Attends relevant meetings and committees of Governing Body.
- Reports regularly to Senior Leadership Team.
- Receives appropriate training and support to fulfil their role effectively.

Responsibilities of Governors

Governors are responsible for ensuring that this policy is reviewed and enforced effectively.

Responsibilities of Head Teacher

The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the e-safety/computing co-ordinator. The Head Teacher and the Deputy Head Teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Responsibilities of classroom based staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices and they participate in annual e-safety training for all staff.
- They have read, understood and signed the school's Acceptable Use Policy (AUP) for staff.
- They report any suspected misuse or problem to the e-safety co-ordinator.
- E-safety issues are embedded in the curriculum and other school activities.

Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Acceptable Use Policies

All members of the school community are responsible for using the school IT systems in accordance with the appropriate Acceptable Use Policy (AUP). AUPs are in place for staff, children (and their parents / carers) and volunteers in school and set out the expectations of all stakeholders when using school IT equipment. As part of their induction, any new member of staff is given the appropriate AUP and current AUPs are reviewed as needed in order to ensure that the policy within reflects the most recent developments in technology. The AUP is discussed with children as part of the e-safety education within the computing curriculum of study and copies are sent home to enable parents / carers to discuss the expectations with their children and support the school in providing a safe learning environment.

There will also be an AUP for visitors to be signed upon entry to school. They will need to sign upon entry to school to ensure e-safety rules are adhered to during the visit. Long term visitors, i.e. school coaches, members of staff from Fellside Fun Club (our wraparound care provider) will be given the same AUP as school staff

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (**those in bold are illegal**) and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **Child sexual abuse images (illegal - The Protection of Children Act 1978).**
- **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003).**
- **Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008).**
- **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986).**
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally the following activities are also considered unacceptable on ICT equipment provided by the school:

- Using school systems to run a private business.
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gambling and non-educational gaming.
- Use of personal social networking sites / profiles for non-educational purposes.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour management procedures.

Email

Access to email is provided for all staff in school via Microsoft Outlook and Office365 email systems. These official school email services may be regarded as safe and secure and are monitored.

- Users need to be aware that email communications may be monitored.
- Users must immediately report, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without their permission.

Use of web-based publication tools

Our school has its own website for sharing information with the community beyond our school. This includes celebrating work and achievements of children. All users are required to consider good practice when publishing content. Personal information should not be posted on the school website. Photographs are posted but never include names alongside an image to identify a pupil. Full names are only used when no image could identify specific pupils.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the e-safety/computing co-ordinator (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system. All users have a responsibility to report immediately to class teachers or the e-safety co-ordinator any infringements of the school's filtering policy in which they become aware or any sites (or apps) that are accessed, which they believe should be blocked. Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Our school filtering is managed and maintained by the local authority who are responsible for blocking, filtering and unblocking any requested websites.

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety curriculum. Staff users will be made aware of the filtering systems through:

- Receiving and agreeing to the AUP and code of conduct
- Briefings in staff meetings, training days, memos etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the AUP and through e-safety awareness sessions / newsletter etc.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The Local Authority, on behalf of the school, will therefore monitor the activities of users on the internet.

E-Safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's computing provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them. E-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of computing lessons and should be regularly revisited – this will cover both the use of IT and new technologies in school and outside school.
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education.
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises. This message will be reinforced through displayed safety rules in each classroom and in the ICT Suite
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT both within and outside school.
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

As a curriculum framework for e-safety, we use that from the '**Education for a Connected World**' (EFACW) (2020 edition) by the UK Council for Internet Safety. The curriculum provision exists for children from Reception to Year 6 and includes the following 8 aspects of online education:

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

- Privacy and security
- Copyright and ownership

Online safety education is a whole school issue. The framework (above) is central to a whole school approach to safeguarding and online safety through improved engagement and the development of an effective curriculum that supports children to be safe, healthy and thriving online. Age-appropriate resources and lesson activities directly linked to the EFCAW framework are utilised via the Project Evolve online toolkit (<https://projectevolve.co.uk/>)

Information literacy

Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

- Cross checking references (can they find the same information on other sites).
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require.

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

Staff Professional Development

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction.
- The e-safety co-ordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority and others.
- All teaching staff have been made aware of this e-safety policy and their responsibility to apply it.
- The e-safety co-ordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

Governor training

Governors will be invited to take part in e-safety training/awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the external providers: National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents.

Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents may sometimes underestimate or not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website.
- Open evenings.
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others
- Drop in sessions/workshops led by the e-safety/computing co-ordinator

Policy Development, Monitoring and Review

This e-safety policy has been developed by a working party made up of:

- E-safety/computing co-ordinator
- Senior Leadership Team

The implementation of this e-safety policy will be reviewed by	The e-safety/computing co-ordinator
Monitoring will take place at regular intervals	Annually.
The governing body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of any e-safety incidents) at regular intervals	Termly via the Head Teacher's Report to Governors
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.	

Related Policies

This policy should be read in association with the following policies:

- Child protection
- Data protection
- Anti-bullying
- Computing

Related Documents

UK Council for Internet Safety (UKCIS) 'Education for a Connected World' (EFACW)
[Education for a Connected World - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

Appendices

Appendix 1

Acceptable Use Policy (AUP) Adults



Acceptable Use Policy for Computers and IT Equipment School Staff

IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. We ask all children, young people and adults involved in the life of Fellside Primary School to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school)

All adults must adhere to the contents of this AUP for **school staff**. Any concerns or clarification should be discussed with the Head Teacher.

- I have read and understood Fellside Primary's full E-Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Online Safety / Headteacher.
- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head Teacher or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that any electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system for school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. **Confidential data will only be stored on an encrypted memory stick.**
- I will not install any hardware or software without permission of the online safety / computing subject leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.



Safer use of technology and the internet

Follow these simple steps to make sure you are safe when using the computer, camera or iPad

The image contains four panels, each with an illustration and a text box. The top-left panel shows a boy pointing to a speech bubble containing icons of a camera, laptop, and tablet with a question mark. The top-right panel shows a girl holding a tablet with a speech bubble containing the 'minimash' logo and a checkmark. The bottom-left panel shows a boy at a computer with a speech bubble containing a question mark and a mouse cursor icon. The bottom-right panel shows a girl looking upset at a computer monitor displaying a red angry face, with a speech bubble containing an exclamation mark.

- ✓ I ask before I use a tablet, computer or camera.
- ✓ I tap or click on things I have been shown.
- ✓ I check if I can tap/click on things I haven't seen before.
- ✓ I tell a grown-up if something upsets me.



Acceptable Use Policy for Computers and IT Equipment Key Stage 2

- I will only use the school computers and IT equipment for purposes I have agreed with a member of staff.
- I will keep my passwords and logins private.
- I will not interfere with anyone else's passwords, logins, settings or files on the computer.
- I will always seek permission before downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
- I know I need permission to take someone's photograph or video them.
- I will not send or forward messages or create material which is deliberately intended to cause upset to other people.
- I will inform a trusted adult if I see or receive any unpleasant material or messages.
- I know I must not give out my personal information (or anyone else's) or arrange to meet with anyone I do not know from online activity (including gaming).
- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
- I understand that if I do not follow these rules, I may not be allowed to use the school computers or access the internet and that this may apply even if the activity happened outside of school.

I have read and understood this Acceptable Use Policy and will agree to follow the statements within it for my own safety and for the safety of others when working online.

Signature:

Print Name:

Date:

Our **Golden Rules** for Staying Safe with Technology and the Internet (KS1 Pupils)

- We only use the Internet when a trusted adult is with us.
- We make sure any messages we send online are always polite.
- We always make careful choices when we use the Internet:
 - We won't share our personal details (our name, where we live, which school we attend etc.);
 - We will only click on pages that our teacher has instructed us to do;
 - Never agree to talk to or meet with strangers we first meet online.
- We always ask a trusted adult if we need help using the Internet.
- We always tell a trusted adult if we find something that upsets us.

I have read and understood this Acceptable Use Policy and will agree to follow the statements within it for my own safety and for the safety of others when working online.

Signature:

.....
.....

PrintName

.....
.....

Date:

.....



SAFE: Always keep personal information safe

MEET: Never arrange to meet up with anyone you meet online

ACCEPTING: Think carefully before you click on a website or download a message

RELIABLE: Remember that not everything that you read online will always be true! Check your information!

TELL: Always tell a trusted adult if something you see

