Fleckney Primary School

E-Safety Policy

Policy drafted by: J Bennett and T Leah

Draft Policy approved by: Headteacher T Leah and Chair of Governors L Marshall

[NB: Final Policy approval on behalf of the Governing Body after consultation.]

Date of review: (bi-annually) Reviewed May 2021

Name of IT Coordinator: J Bennett

E-Safety Policy

The Importance of E-safety

Computing and the use of digital devices is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Pupils use the internet widely outside of school and, consequently, we as a school need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Podcasting
- Coding
- Gaming
- Mobile devices
- Video & Multimedia

What is E-safety?

E safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's E safety policy will operate in conjunction with other policies including the Acceptable use of IT for staff and pupils, child protection, behaviour, health and safety, anti-bullying and PHSE.

Roles and Responsibilities

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads.

Key staff:

- Designated Safeguarding Lead (DSL) team – Mr T Leah, Mrs S Allen, Miss E Pearson

E-safety involves pupils, staff, governors and parents making best use of technology, information and training to create and maintain a safe online and ICT environment our School.

Headteacher: Mr T Leah

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

DSL team: Mr T Leah, Mrs S Allen, Miss E Pearson

Key responsibilities:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns

- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety – the new LGfL DigiSafe pupil survey of 40,000 pupils may be useful reading (new themes include 'self-harm bullying' and getting undressed on camera)
- Reviewand update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online safety education is embedded across the curriculum(e.g. by use of the UKCISframework 'Education for a Connected World') and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware
- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are Mr T Leah, Mrs S Allen, Miss E Pearson.

- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL/DDSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices,the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/DDL know
- Receive regular updates from the DSL/DDSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe pupil survey of 40,000 pupils (new themes include 'self-harm bullying' and getting undressed on camera)
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

Managing the school e-safety messages

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

E-safety guidelines and the SMART rules will be prominently displayed around the school.

As a school, each year, we also participate in e-safety activities during Safer Internet Day.

What are the Risks?

The internet is a fantastic resource we can use to enhance learning. It has many benefits, however, we must also be aware of the risks that come with it.

Some of the dangers children may face include:

- 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
- Cyberbullying
- 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 the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The E safety policy that follows explains how we intend to do this.

E-safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

All internet activity within school is monitored and filtered through 'Netsweeper'. Whenever any inappropriate use is detected, the ICT Coordinator and DDSL or DSL is notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's digital devices.

If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

Infrastructure

Our internet access is provided by EMPSN.

LEAMIS support the administrative devices throughout school and curriculum access is managed by the school's ICT Coordinator.

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, e-safety co-ordinator (ICT coordinator), and the Designated Safeguarding Leads.

Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing email

The use of email within school is an essential means of communication for staff.

Pupils currently do not access individual email accounts within school.

Staff must use the school's approved email system for any school business.

Staff must inform (the ICT Coordinator and Designated Safeguarding Leads) if they receive an offensive or inappropriate e-mail.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images

Creation of videos and photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case. If mobile phones are used on occasions for photos, this should first be discussed with the Head Teacher and the images must be down loaded to the school site and then removed from the staff member's phone.

Publishing pupil's images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw or amend permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school based publicity materials.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops.

Complaints

Complaints or concerns relating to e-safety should be made to the Headteacher or a member of the DSL team.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT coordinator and the designated safeguarding leads.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by the class teacher and then forwarded to the e-safety co-ordinator. Depending on the seriousness of the offence; investigation maybe carried out by the Headteacher or LA. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Equal Opportunities

Pupils with additional needs

The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Internet activities are planned and well-managed for these children and young people.

Concerns about a child

Online safety concerns follow the same procedure as any other safeguarding concerns: