FRONT STREET COMMUNITY PRIMARY SCHOOL

ESAFETY POLICY:
GUIDANCE
September 2024

SCHOOL WIDE

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.

The school identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content. For example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact**: being subjected to harmful online interaction with other users. For example, peer on peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. 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:

At Front Street Primary we adopt a whole school approach to online safety which will empower, protect, and educate our learners and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate. We 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. We will ensure online safety is reflected as required in all relevant policies and 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:

The DSLs (Helen Gladstone and Martyn Kelly) have overall responsibility for online safety within the school, but will liaise with other members of staff such as Jess Carter (computing lead) and Karen Robinson (Computing HLTA) as necessary.The e-safety coordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. We recognise that technology, and the risks and harms related to it, evolve and change rapidly. Therefore, the e-safety coordinator will carry out an annual review of our approaches to online safety.

- 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 (CPOMS) 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 associated policies such as anti-bullying policy, social media policy and behaviour policy.
- They report any suspected misuse or problem to a member of the Senior Leadership Team.
- E-safety issues are embedded in the curriculum and other school activities.

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 Management Team

The implementation of this E-Safety Policy will be reviewed by	The E-Safety / Computing Coordinator.
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.	

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:
At Front Street, we use a wide range of technology. This includes computers, laptops, Chromebooks, i-Pads and other digital devices, the internet, our learning platform, intranet and email systems.

- All school owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. This appears on all login screens for staff/children to accept before use.

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.

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.
- The use of AI (Artificial intelligence) tools in or out of school to cause harm to pupils or staff.

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.

Use of hand-held technology (personal phones and hand-held devices):

We recognise the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras and wearable technology. In accordance with KCSIE 2024 the school has appropriate mobile and smart technology, image use, online and acceptable use policies in place, which are shared and understood by all members of the community. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. Devices should only be used by members of staff in areas not accessed by pupils and only when not in contact with pupils. Staff can, however, request permission to keep a phone switched on in certain circumstances (e.g. an expected and important phone call).
- Mobile phones must be kept securely out of the view of pupils unless when being used in the above areas.
- Staff should never use their own personal mobile devices to take or store photographs of children at school events, sporting trips or excursions. Only authorised school cameras and iPads can be used to record videos or images of school events.
- Older pupils are permitted to bring their personal hand-held devices into school with the agreement of parents (usually to facilitate the process of children beginning to walk home alone). All pupil phones are kept locked away during the school day and are collected by children before they leave.
- In line with KCSIE 2024 - staff should also be aware of acceptable use on line in and out of school.

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 school website, Facebook page and YouTube Channel, 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.

Appropriate Filtering and Monitoring
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. 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.

- We will do all we reasonably can to limit children's exposure to online risks through school provided IT systems and will ensure that appropriate filtering and monitoring systems are in place.
- Our school filtering is managed and maintained by the local authority who are responsible for blocking, filtering and unblocking any requested websites.
- All users have a responsibility to report immediately to class teachers / E-Safety / Computing Coordinator any infringements of the school's filtering policy of which they become aware or any sites 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.
- All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation.
- Pupils are made aware of the importance of filtering systems through the school's E-Safety Education Programme.

- Staff will be regularly kept up to date with filtering processes, through 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 Acceptable Use agreement and through E-Safety awareness sessions / newsletter etc.

If staff discover unsuitable sites or material, they are required to notify the e-safety lead/DSL in order to alert Gateshead Authority as soon as possible. Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the Internet Watch Foundation and the police. When implementing appropriate filtering and monitoring, we will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

We acknowledge that whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety.

- Children will use appropriate search tools, apps and online resources as identified following an informed risk assessment.
- Children's internet use will be supervised by staff according to their age and ability.
- Children will be directed to use age-appropriate online resources and tools by staff.

The Use of Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access and generative chatbots such as ChatGPT and Google Bard may be familiar with adults and children. The use of AI can have a positive impact on the way pupil's learn but there is also a potential risk for it to be used in a harmful way. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. All school staff have had Safeguarding training and have been made aware of the risks of using AI tools. Any use of it to bully pupils will be dealt with in line with our school behaviour policy. Teaching staff are not permitted to use AI for teaching and learning purposes without expressed permission from the headteacher.

Information Security and Access Management

- School is responsible for ensuring an appropriate level of security protection procedures are in place, in order to safeguard our systems as well as staff and learners. Further information can be found in:
  - E-safety Policy
  - Safeguarding Policy
  - acceptable use policy (on devices at login)
  - Safe use of internet and email policy
- We will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

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 is provided. One lesson will be delivered half termly as part of Computing lessons. Topics should be regularly revisited – this will cover both the use of IT and new technologies in school and outside school. Overview of topics can be seen on the Whole School Online Safety Overview document.
- The e-safety programme will be delivered throughout the whole school year (not blocked within one term) and carefully scheduled throughout the year to ensure themes are readdressed at times where it may be more common for children to have access to devices e.g. Christmas.
- We supplement our E-safety teaching with the resources on CEOP's Think U Know site as part of 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.
- 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.
- E-safety is addressed through other subjects, such as part of the PSHE curriculum.

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).
- Older 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. Pupils play a part in monitoring this policy.

Staff Professional Development:

It is essential that all staff receive e-safety training (via the National Online Safety Hub) 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 Coordinator 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 / Computing Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.
- Staff will be required to check in regularly to the National Online Safety Hub, and watch training videos to support with CPD.

Governor training:

Governors should 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.
- Have access the National Online Safety hub, and take part in training videos.

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. We therefor build a partnership approach to online safety and will support parents/carers to become aware of and alert to the potential online benefits and risks for children by:

- Regular and up to date information, including links to e-safety websites on letters, newsletters, web site.
- Open evenings for parents to find out more information.
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others
- Drop-in sessions led by the E-Safety / Computing Co-ordinator.

Remote Learning

Specific guidance for DSLs and SLT regarding remote learning is available at DfE: **Safeguarding and remote education during coronavirus (COVID-19)** and The Education People: **Remote Learning Guidance for SLT.**

- We will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with children and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and Google Classroom.
- Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and children will engage with remote teaching and learning in line with existing behaviour principles as set out in our behaviour policy/code of conduct and Remote Learning policy.
- Staff and children will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will follow our remote learning policy.
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. We will continue to be clear who from the school their child is going to be interacting with online (class teacher/class teaching assistant).

- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety