Pinfold Online Safety Policy

Head: Claire Gagigo

Chair of Governors: Sue Kenny

Claire Gagigo 2023

Pinfold Curriculum intent:

We believe children have an unlimited capacity for learning and personal success: our challenging and inspiring 'Faraway Curriculum' will create independent, critical thinkers, confident, responsible and caring; high reaching learners, who can see the magic in our world. They will gain the skills, knowledge and strength of character to be able to keep themselves and others safe and happy, challenge discrimination and make our world a better place.

Impact and Review

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Internal monitoring data for network activity
- Surveys / questionnaires of
- students
- parents / carers
- staff
- This policy will be updated in accordance with any legal requirements and guidance form LCC or the DFE as and when necessary and reviewed annually

This policy works in conjunction with our:

- Positive Behaviour Management and Behaviour for Learning policy
- Diversity and Equality Policy
- ICT Acceptable Use Policy
- Home School Agreement
- Child Protection and Safeguarding Policy
- KCSIE 2023

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. 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.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

• regular meetings with the E-Safety Co-ordinator

• regular monitoring of e-safety incident logs

• regular monitoring of filtering / change control logs

• reporting to relevant Governors / Board / committee / meeting

Headteacher and Senior Leaders:

• The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is everyone's.

• The Headteacher and (at least) another member of the Senior Leadership Team 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.

• The Headteacher / Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

• The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Technical staff (EDS Educational Digital Services):

Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

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
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; E-Safety Coordinator for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices in lessons where internet use is pre-planned students 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.

Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

Students:

• are responsible for using the school digital technology systems in accordance with the ICT Acceptable Use Policy

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

• their children's personal devices in the school

Teachers and parents and carers

Teachers and parents and carers can help their children stay safe on line by:

Teaching children how to evaluate what they see online - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable. Schools can help pupils consider questions including:

• is this website/URL/email fake? How can I tell?

• what does this cookie do and what information am I sharing?

• is this person who they say they are?

• why does someone want me to see this?

• why does someone want me to send this?

• why would someone want me to believe this?

• why does this person want my personal information?

• what's behind this post?

• is this too good to be true?

• is this fact or opinion?

Teach our children how to recognise techniques used for persuasion – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others.

Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

We can help children to recognise:

• online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),

• techniques that companies use to persuade people to buy something,

• ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and

• criminal activities such as grooming.

Online behaviour –

This will enable children to understand what acceptable and unacceptable online behaviour look like. We should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. We should also teach pupils to recognise unacceptable behaviour in others. We can help pupils to recognise acceptable and unacceptable behaviour by:

• looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,

• looking at how online emotions can be intensified resulting in mob mentality (peer group pressure),

• teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and

• considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

We can help pupils to identify and manage risk by:

• discussing the ways in which someone may put themselves at risk online,

• discussing risks posed by another person's online behaviour,

• discussing when risk taking can be positive and negative,

• discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations,

i.e. how past online behaviours could impact on their future, when applying for a place at university or a job for example,

How and when to seek support – This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online. Schools can help pupils by:

• helping them to identify who trusted adults are,

• helping them to understand that various platforms and app

Sexual harassment

As set out in KCSIE, sexual violence and sexual abuse can happen anywhere, and all staff working with children are advised to maintain an attitude of 'it could happen here'.

Schools and colleges should be aware of, and respond appropriately to all reports and concerns, including those outside the school or college, and or online. Schools and colleges should be aware of the importance of:

• making clear that there is a zero-tolerance approach to sexual violence and sexual harassment and it is never acceptable, and it will not be tolerated and it should never be passed off as "banter", "just having a laugh", "part of growing up" or "boys being boys". Challenging physical behaviour (potentially criminal in nature), such as grabbing bottoms, breasts and genitalia, pulling down trousers, flicking bras and lifting up skirts. Dismissing or tolerating such behaviours risks normalising them; and

• not recognising, acknowledging or understanding the scale of harassment and abuse and/or downplaying some behaviours related to abuse as it can lead to a culture of unacceptable behaviour, an unsafe environment and in worst case scenarios a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it; and

• understanding that all of the above can be driven by wider societal factors beyond the school and college, such as everyday sexist stereotypes and everyday sexist language. This is why a whole school/college approach (especially preventative education) as described in Part 3 (KCSIE) of this advice is important.

We are aware that children with Special Educational Needs and Disabilities (SEND) are three times more likely to be abused than their peers. Additional barriers can sometimes exist when recognising abuse in SEND children. It is particularly important to be vigilant when a child has SEND.

- Peer on Peer Abuse is now referred to as Child on Child, this can occur in real life and online'

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.