Kilby C of E Primary School

Online Safety Policy KCSiE

Contents

Development / Monitoring / Review of this Policy 2
Scope of the Policy 2
Roles and Responsibilities 3
- Governors 3
- Headteacher 3
- Online Safety Coordinator 4
- Network Manager / Technical staff 5
- Teaching and Support Staff 5
- Designated Safeguarding Lead 6
- Pupils 6
- Parents / Carers 6

Policy Statements 7
- Education – Pupils/Teaching Staff 7
- Education – Parents/Carers 8
- Education & Training – Staff/Volunteers 8
- Technical – infrastructure / equipment, filtering and monitoring 8

Use of digital and video images 9
Communications 10

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by:

- Head Teacher
- Online Safety Coordinator

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	**Insert Date Here**
The implementation of this Online Safety policy will be monitored by:	**Headteacher / SLT / Online Safety Coordinator**
Monitoring will take place at regular intervals:	**Annually**
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	**Annually**
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	**July 2025**
Should serious online safety incidents take place, the following external persons / agencies should be informed:	**Headteacher / Online Safety Coordinator / Chair of Governors / LADO / Social Care / Police**

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers and/or visitors) who have access to and are users of school digital technology 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 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 online-bullying or other Online 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.

The school will deal with such incidents within this policy and associated behaviour, anti-bullying and safeguarding policies and will, where appropriate, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for reviewing all aspects of children's safety and well-being in school including the Online Safety Policy.

In accordance with Keeping Children Safe in Education 2024 (KCSiE2024), which comes into force in September 2024, and government guidance on filtering and monitoring standards, governing bodies have overall strategic responsibility – alongside the Headteacher – for filtering and monitoring. They must ensure that a senior member of staff and a governor have been assigned responsibility of ensuring that filtering and monitoring standards are met and that there is clarity on the role and responsibilities of staff and third parties, including external IT service providers. Standards of filtering and monitoring should be in line with 'Meeting digital and technology standards in schools and colleges' guidance provided by the government.

In accordance with KCSiE2024, governing bodies should ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated. Induction and training should be in line with any advice from the safeguarding partners.

Headteacher

- has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Coordinator.
- should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- is responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- in accordance with KCSiE2024 and government guidance on filtering and monitoring standards, the Headteacher (alongside the governing body) has responsibility for filtering and monitoring. They must ensure that a senior member of staff and a governor have been assigned responsibility of ensuring that filtering and monitoring standards are met and that there is clarity on the role and responsibilities of staff and third parties, including external IT service providers.
- the Headteacher is responsible for procuring filtering and monitoring systems, documenting decisions on what is blocked and why, reviewing the effectiveness of provision and overseeing reports. This must also be informed by the school's response to the Prevent Duty.
- the Headteacher is responsible for making sure that all staff understand their role, are appropriately trained, act on reports and concerns, and follow policies, processes and procedures. In accordance with KCSiE2024, the Headteacher should ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated. Induction and training should be in line with any advice from the safeguarding partners.

- the Headteacher should work with governors and DSLs to make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information. This review should be at least annually, but it may also take place at other points, such as when a safeguarding concern is raised, there is a change in working practices, or if new technology is introduced. As part of this review, checks of filtering provision need to be completed and recorded. These checks should be undertaken from both a safeguarding and IT perspective.
- the Headteacher should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.
- the Headteacher will ensure that the school's approach to online safety is reflected in the child protection policy. This will include, amongst other things, appropriate filtering and monitoring on school devices and school networks and a clear policy on the use of mobile and smart technology. This policy should reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks and that this access means that some children may sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) or view and share pornography and other harmful content.
- the Headteacher will work with IT providers to ensure the appropriate level of security protection procedures are in place in order to safeguard systems, staff and learners, and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Online Safety Coordinator

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- liaises with SLT to develop, implement and monitor a whole school online safety curriculum
- ensures the school website contains up-to-date and relevant information regarding online safety for both parents and children.
- provides training and advice for staff.
- liaises with school technical staff.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- reports to Governors as required.

Network Manager / Technical staff

The Headteacher and their designated service 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 online safety technical requirements.
- that users may only access the networks and devices through a properly enforced password protection policy.
- the filtering protocols are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they, and the online safety coordinator, keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network and online services provided by school is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation.
- that monitoring software / systems are implemented and updated as required.

Teaching and Support Staff

Are responsible for ensuring that:

- they are aware that KCSiE2024 highlights the use of technology as a significant component in many safeguarding issues, and that they have a responsibility to be aware of the school's filtering and monitoring procedures and practices.
- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- they have read, understood and signed the documents relating to staff conduct and the acceptable use of internet.
- they report any suspected misuse or problem to the Headteacher/Online Safety Coordinator for investigation / action / sanction.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- they implement the online safety curriculum (delivered through the Computing curriculum) and ensure online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Online Safety Policy as summarised by the child-friendly SMART Rules.
- through the curriculum, pupils 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, pupils should normally 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 Online 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
- online-bullying

The DSL should work closely with IT service providers to meet the needs of the school.

The DSL (with support from deputy DSLs) should take lead responsibility for safeguarding and online safety and should work collaboratively with the Headteacher on filtering and monitoring reports, safeguarding concerns, and checking filtering and monitoring systems.

Pupils

- are responsible for taking care of school equipment and using the school digital technology systems in accordance with the SMART Rules
- have a good understanding of research skills and the need to avoid plagiarism
- 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 safe rules for using mobile devices and digital cameras. They should also know and understand safe rules for taking / use of images and online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and SMART Rules cover 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, including by maintaining a website page containing up-to-date and relevant information and resources. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Policy Statements

Education – Pupils/Teaching Staff

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 online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of regular assemblies and classroom sessions – including in the weeks before school holidays
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making.
- Pupils should be helped to understand the need for the SMART Rules and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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, that school leaders are confident filtering is in place 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, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. School will support parents and carers in developing an understanding of how they can fulfil this role effectively. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

- The school will therefore seek to provide information and awareness to parents and carers through:
- Curriculum activities
- Letters, newsletters and the school website
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day & Anti-Bullying Week
- Links on the school website

Education & Training – Staff/Volunteers

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

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements and their importance in safeguarding children in and out of school.
- It is possible that some staff may identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and/or by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.
- Staff will be given opportunities to access relevant training materials on the Educare training platform and through period staff briefings

Technical – infrastructure / equipment, filtering and monitoring

IT Contractors and the school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers to use photographs of children on the school website and other publications is obtained when a child joins school.
- In accordance with guidance from the Information Commissioner's Office, parents / carers may be invited to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images. This is at the Headteacher's discretion, and the Headteacher may not allow any parents to take photographs as part of safeguarding practices.
- Staff and volunteers are allowed to take digital / 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 taken on school equipment, the personal equipment of staff should not be used for such purposes, unless consent has been obtained in advance from the Headteacher and another staff member is present. Images should be deleted asap, normally within 24 hours, if taken on a personal device.
- 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
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications should typically take place on official (monitored) school systems.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.