Killigrew Primary & Nursery School

Online Safety Policy

(including acceptable use agreements)

March 2024

Contents

1. Introduction

Killigrew Primary and Nursery School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. We are, therefore, committed to ensuring that all pupils, staff and governors are supported to use internet, mobile and digital technologies safely. This is a key part of our safeguarding responsibility. We know that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.

- The named online safety lead in this school is M. Lockwood.
- All breaches of this policy must be reported to T. Mylotte.
- All breaches of this policy that may have put a child at risk must also be reported to one of the DSLS: T. Mylotte, K. Morley, K. Norris and M. Wicks and details of the incident recorded promptly on CPOMS.

Organisations that are renting space from the school and are a totally separate organisation follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or digital equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to (a non-exhaustive list):

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- work placement students
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers through the website, social media, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked, but not limited to, to the following other school policies and documents:

- Child Protection Policy
- Keeping Children Safe in Education 2023-2024
- Prevent duty
- GDPR
- Health and Safety Policy
- Killigrew home–school agreements
- Remote learning policy
- Behaviour policy
- Anti-bullying policy
- PSHE curriculum and policies
- Staff code of conduct

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

<u>Use of email</u>

Staff and governors use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication.

Staff must not contact pupils, parents or conduct any school business using a personal email address or social media account. The only exception to this is when a parent needs to be contacted in an emergency when offsite on a trip or sporting fixture out of usual school hours (i.e. nobody arrives to collect a child). In this situation, Mrs Morley and/or Miss Mylotte must be notified.

Pupils use school approved accounts on the school system for educational purposes. Where required, parent/carer permission is obtained for the pupil account to exist. Our GDPR policy provides full details on information linked to sharing personal or confidential information and the need to gain appropriate permissions. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Miss Mylotte.

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. This includes personal responsibility for running videos from YouTube through a 'safe share' system prior to use.

- Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the School Business Manager with details of the site/service and seek approval from Mrs Morley. The terms and conditions of the service are adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites suggested must have been checked by the teacher.

- All users must observe copyright of materials from electronic sources. This includes all images that are used on the school website.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content.

- When working with pupils searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:
Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

Users must not:

- Reveal or publicise confidential or proprietary information.
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses.
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school.
- Use the school's hardware and Wi-Fi facilities for running a private business.
- Intimidate, threaten or cause harm to others.
- Access or interfere in any way with other users' accounts.
- **Use another user's account and password.**
- **Leave their equipment or digital media logged in so that others (adults and children) could access sensitive or confidential information. When leaving their workstation, their desktop must be locked or logged out.**
- Use software or hardware that has been prohibited by the school.

Only a school device may be used to conduct school business outside of school. This could and might include, but is not limited to, iPads, Chrome Books, desktop computers and other electronic devices (for example Kindle Fires). The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by T. Mylotte.

<u>Storage of Images</u>

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be

changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include cloud-based services. Staff have access to the photographs taken, but only when accessed on the secure network. Photos are deleted after the pupil has left the school, in line with the GDPR policy.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. This includes recording pupil voice.

Use of personal mobile devices

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities.

Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child unless there is a pre-specified permission from T. Mylotte.

When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Pupils in Year 6 are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes on school premises (including before and after school). Year 5 are allowed to bring in phones in the summer term (following the same guidelines as noted here). Phones must be handed to the class teacher at the start of the day and collected at the end of the day. Phones must be stored out of reach in a cupboard. All phones must be on silent.

Under no circumstance should pupils use their personal mobile devices/phones to take images of any other pupil unless they and their parents have given agreement in advance or any member of staff.

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

Personal mobiles/devices must never be used to access school data or SharePoint. They can be used to access emails, but only if the mobile device has the appropriate security: either face recognition or a 6-digit passcode. The device must be locked when not in use.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out a risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with T. Mylotte before they are brought into school.

Smart watches and similar devices

The school allows staff, including temporary and peripatetic staff, and visitors to wear smart watches and it is recognised that a smart watch may be visible on an adult's wrist. However, when in the presence of pupils, they must be in silent mode, with camera, messaging and call services disabled. In designated areas and not in the presence of pupils, full functionality can be restored.

Pupils are not allowed to wear smart watches to school. If they are in possession of a smart watch, the watch will be confiscated and returned to the parent/carer.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff. This member of staff must notify Mr Lockwood in the first instance. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

Filtering and Monitoring

Schools and colleges must provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Governing bodies have overall strategic responsibility for filtering and monitoring and must seek assurance that the standards are being met.

Miss T. Mylotte and other senior leaders are accountable for the following responsibilities, working closely with the schools IT service provider (Herts for Learning):

- procuring filtering and monitoring systems.
- documenting decisions on what is blocked or allowed and why.

- reviewing the effectiveness of provision.
- overseeing reports.
- making sure that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.

Miss T Mylotte and Mrs K Morley also take lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports.
- safeguarding concerns.
- checks to filtering and monitoring systems.

Our IT service provider has technical responsibility for:

- maintaining filtering and monitoring systems.
- providing filtering and monitoring reports.
- completing actions following concerns or checks to systems.
- working with the school to procure systems, identify risk and carry out reviews and checks.

Annual Review

To understand and evaluate the changing needs and potential risks, our filtering and monitoring provision is reviewed at least annually. The review is conducted by Miss T Mylotte together with the IT service provider and Mr G Fry (chair of governors). The results of the online safety review are recorded for reference and available to those entitled to inspect that information.

For this review, the following criteria are considered:

- the risk profile of pupils, including their age range, pupils with SEND and pupils with English as an additional language (EAL).
- what the filtering system currently blocks or allows and why.
- any outside safeguarding influences, such as county lines.
- any relevant safeguarding reports.
- the digital resilience of pupils.
- The teaching within the E-safety, RHSE and PSHE curriculum
- the specific use of chosen technologies.
- related safeguarding or technology policies.
- what checks are currently taking place and how resulting actions are handled.

The review will inform the following documents and processes:

- related safeguarding or technology policies and procedures.
- roles and responsibilities.
- training of staff.
- curriculum and learning opportunities.

- procurement decisions.
- how often and what is checked.
- monitoring strategies.

The review will be done as a minimum annually, or when a safeguarding risk is identified, there is a change in working practice or new technology is introduced.

Checks to filtering provision are completed and recorded as part of the filtering and monitoring review process. Checks are undertaken from both a safeguarding and IT perspective. The checks include a range of school owned devices and services, including those used off site, and checks of different user groups, for example, teachers, pupils and guests.

There is a log of the checks which records –

- when the checks took place.
- who did the check.
- what they tested or checked.
- resulting actions.

All staff know how to report and record concerns and filtering and monitoring systems are checked on new devices and services before releasing them to staff and pupils. Blocklists are reviewed and modified in line with changes to safeguarding risks.

An active and well managed filtering system is an important part of providing a safe environment for pupils to learn. No filtering system can be 100% effective so it is important to understand the coverage of the filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet the statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty.

An effective filtering system needs to block internet access to harmful sites and inappropriate content, but it should not unreasonably impact teaching and learning or restrict pupils from learning how to assess and manage risk themselves. Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. Therefore, our IT filtering provider facilitates system specific training and support for senior leaders.

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing prompt action and recording. Using a variety of monitoring strategies, enables safeguarding risks on internet connected devices to be minimised. These strategies may include:

- physically monitoring by staff watching screens of users.
- live supervision by staff on a console with device management software.
- network monitoring using log files of internet traffic and web access.
- individual device monitoring through software or third-party services

The governing body supports the senior leadership team to review the effectiveness of monitoring strategies and reporting process. They check that incidents are urgently picked up, acted on and outcomes are recorded.

Device monitoring needs to -

- check that monitoring systems are working as expected.
- provide reporting on pupil device activity.
- ensure that monitoring data is received in a format that staff can understand.
- identify users, so concerns can be traced back to an individual, including guest accounts.

5. Curriculum

Online safety is fully embedded within our curriculum and our teaching is supported through our Project Evolve scheme of work. This provides a comprehensive age-appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity.

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment.

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives), understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online.

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B)

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix E).

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. The Acceptable Use Agreement explains the

school's expectations and pupil and parent/carer responsibilities.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported using the school's E-Safety log.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

The Safeguarding Lead Governor- Mr G Fry (chair of governors) receives termly summary data on recorded online safety incidents for monitoring purposes. In addition, all governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.