Linton CE Infant School

Online Safety Policy

Date: February 2026

Review Date: February 2027

Background to this policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age-appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

Online safety in schools is primarily a safeguarding concern and not a technology one. Therefore, this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- **Safeguarding and Child Protection**
- **Safer Working Practices**
- **Data Protection / GDPR Policy**
- **Policy for use of Artificial intelligence in school**
- **Anti-Bullying Policy**
- **School Complaints Procedure**
- **Cambridgeshire Progression in Computing Capability Materials**
- **Whistle Blowing Policy**

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- **The Headteacher**
- **The Designated Safeguarding Lead**
- **The Computing Subject Leader**

- This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email and is readily available on the school network and website and has also been made available to parents..

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As online safety is an important part of our school's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale

At Linton CE Infant School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the misuse of technology can put users of technology at risk within and outside the school.

The risks they may face can broadly be categorised into the 4 C's; **Contact**, **Content**, **Conduct, and Commerce** (Keeping Children Safe in Education 2022) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- 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, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- Phishing or financial scams
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops / iPads / desktops - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Staff / some staff have access to school systems beyond the school building (e.g. MIS systems, Microsoft 365.
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- Staff level internet access
- All staff have access to Class Dojo
- Some staff have access to the school Facebook account.
- Some Staff have access to online learning platforms Purple Mash, Collins Hub, Little Wandle phonics and Charanga music

Pupils:

- Curriculum laptops / iPads including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources

- Cloud platforms / online tools providing pupils with access within and beyond the school gates including Class Dojo, Collins Hub and Purple Mash.

Where the school changes the use of existing technology or introduces new technologies which may pose risks to users' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The online safety curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing (England) and the statutory Relationship and Health Education.

At Linton CE Infant School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

Our online safety curriculum is based on the Cambridgeshire Progression in Computing Capability Materials, and Project Evolve, with reference to UKCIS's Education for a Connected World. *We also use 2Simple, 2BeSafe resources as part of the lessons.*

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.
- Focus events to raise the profile of online safety for our pupils and school community
- A flexible curriculum which is able to respond to new challenges as they arise.

Continued professional development

In accordance with KCSiE guidance, staff at Linton CE Infant School receive safeguarding and child protection training at induction. This training covers online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. Safeguarding, child protection and online safety training is regularly updated during staff meetings and through updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

Linton CE Infant School will identify a member of the senior leadership team and a governor, to be responsible for ensuring the DfE filtering and monitoring standards are met. These identified individuals will receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Monitoring and averting online safety incidents

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include:

- Secure, private BT internet connection. This is provided and maintained BT.
- The use of Smoothwall as Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites.
- Antivirus package provided as part of BT Connection and support from ICT services.

Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies

Staff use of the schools' internet can also be monitored and investigated where needed.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.
- Pupils have class logins to the school network.
- All pupils have individual, password protected logins to class dojo, Purple Mash, Collins Hub and other online resources.
- Visitors to the school can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case-by-case basis.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

Responding to online safety incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.

If an online safety incident occurs, Linton CE Infant School will follow its agreed procedures for responding, including internal sanctions and involvement of parents (this may include the deactivation of accounts, restricted access to systems as per the school's AUPs or reporting incidents to the police and other authorities – see appendix 1: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure).

In addition, 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 cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk and it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

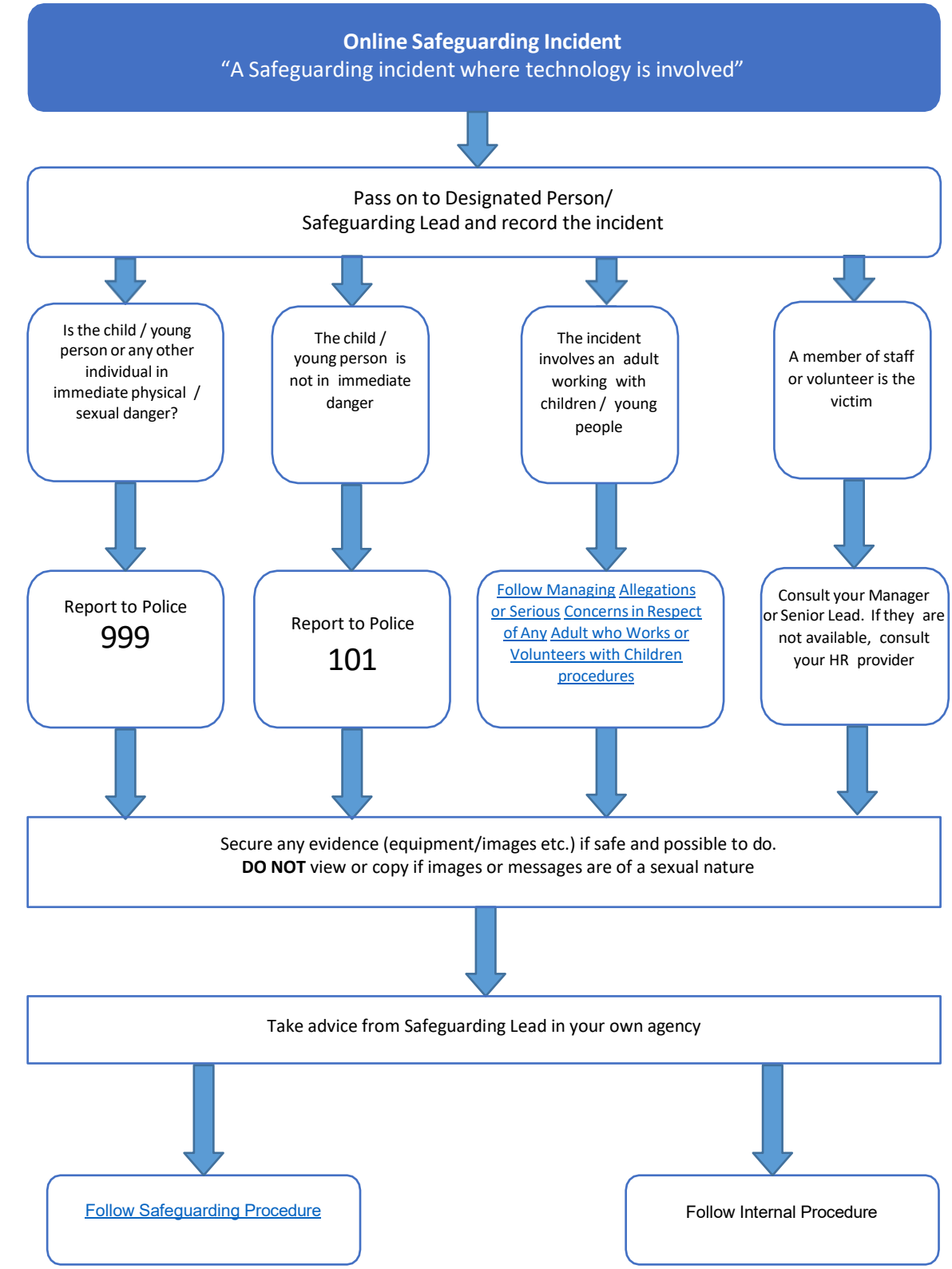
NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Appendix 1: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure

Where the school suspects that an incident may constitute a safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.

If you think that a child or young person is at risk of serious harm contact Children Social Care https://safeguardingcambspeterborough.org.uk/concerned/

Out of hours emergencies 01733 234724.



Throughout this process, please ensure that all those involved are supported appropriately

Appendix 2

Staff AUP

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system and other technology in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this agreement.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Use of school based equipment

When using the school's ICT equipment and other information systems, staff should ensure that they have understood and will comply with the following statements

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety coordinator.
- I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords and will ensure that these are kept securely.
- I will seek consent from the computing lead/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the computing lead/ headteacher.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the computing lead.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information (UK GDPR).
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will use OneDrive cloud solution to store data that I wish to work on off site and understand that this is a secure system protected by secure login details.
- If portable storage devices are necessary, I will only use school-owned or provided portable storage (USB sticks, SSD cards, portable hard drives etc) to transport any sensitive data.
- I will ensure that any personal or sensitive information taken or worked on off site will be saved within my professional personal OneDrive cloud solution (preferably) or on a school-owned storage device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset (For example spread sheets/other documents created from information located within the school information management system) which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network or on

OneDrive cloud space and access controlled in a suitable manner in accordance with the school data protection controls.

- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the computing lead/Headteacher.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at any time to protect my own and others' safety, and action may be taken if deemed necessary to safeguard others or myself.
- I understand that if I leave the employment of Linton CE Infant School, data in my work area will be held for **1 year** then deleted.
- I will not store personal information on the school network or access websites that require personal information (such as payment details) on the school network.

Social Networking

- I will take care when using personal social media such as Facebook, Twitter, and YouTube or any other online publishing websites to not discuss my professional role in anyway which could disclose sensitive information.
- I will not use social networking tools such as WhatsApp, messenger or snapchat to communicate with parents about my professional role.
- I will not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents about my professional role unless approved in writing by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff should not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues, or my professional status, I will take screenshots for evidence and escalate to the computing lead/designated safeguarding lead.
- When absent from school (sickness or during school holiday periods) I will use my professional judgement as to what is appropriate to publish online.
- I will not create a social networking profile, blog or account and use it for school purposes without prior written authorisation from SLT.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved.
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright licencing.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and deleted as soon as possible from the device memory or memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues

and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- I will use my school email address for correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will not use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and if necessary, authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.
- When replying to group emails I will ensure that I will only use the 'reply all' function when it is strictly necessary.

Class dojo

- I understand that Class dojo is a professional tool for communication with parents and will ensure that messages and posts are written in a professional manner. Messages should be model polite and professional communication.
- I will ensure class dojo messages will be written carefully and, if necessary, checked and authorised before sending to ensure I protect myself.
- I will ensure that photographs uploaded to class and school story do not feature children for whom we do not have permission to use photographs (see list) or staff who have not given their permission.
- I will ensure that messages from parents are replied to in a timely manner.
- I will ensure that any messages received from parents are shared with the child's class teacher or senior leadership team where necessary.
- I understand that the senior leadership team discourage the use of class dojo on any personal devices.
- I will follow the flowchart guidance regarding uploading posts to Class dojo. See appendix A

Microsoft Teams and 365 cloud solutions

- I understand that Microsoft Teams is a professional tool to be used amongst the staff team and with other professionals and as such messages should be written in a professional manner. Messages should be model examples of polite and professional communication.
- I will ensure messages I receive are replied to promptly.
- I understand that Microsoft teams will be used for online staff meetings and I will ensure that my login details and account are kept secure and used only by myself for professional activities relating to school.
- If using Teams to meet virtually with parents I will ensure that the meeting link is shared via a message on class dojo in a timely manner and not sent directly to a parent's personal email account.
- I understand in using Teams I can share and collaborate on documents and save documents to a cloud solution.

Mobile phones and devices

- Personal mobile devices will be stored securely in bags, lockers or cupboards during teaching time unless specified otherwise by the senior leadership team.
- I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode during school hours.

- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team under specific circumstances.
- I understand that the senior leadership team discourage the use of personal mobile devices to access school email or class dojo.
- Under no circumstances will I use any personally owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team. Any images or sounds recorded with permission should be uploaded to a school device and deleted form the device and any cloud-based photo storage i.e. iCloud, google photos immediately.
- I will not contact any parents or pupils on my personally owned device unless permission is explicitly given by the senior leadership team.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach age an appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Agreement

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name :
Role in School:
Signed
Date:

Appendix A

To ensure that Class dojo remains a useful and efficient tool for sharing information all staff should follow the following guidance when uploading posts.

Type of post	Content	Guidelines
Individual portfolio	Mainly used for learning journey posts in EYFS and possibly year 1 and 2.	Used only in year 1 and year 2 with prior agreement from class teacher.
Class story posts	Posts about learning going on in class Class specific events and information sharing. Messages specific to individual class	Posts uploaded after prior agreement from the class teacher leading the class for the lesson. No videos of teaching to be uploaded.
School story posts	Events information for parents i.e. led by subject leaders Administrative posts Headteacher posts	Posts should only be uploaded after prior agreement from Kelly
Messages to parents		Contents of messages should be shared with class teacher when necessary.

Appendix 3

Staff Acceptable Use Agreement

Use of Artificial Intelligence

Emerging technologies, including Artificial Intelligence (AI), are increasingly integrated into educational settings and the lives of staff and learners. These technologies have immense potential to enhance creativity, promote personalized learning, and improve operational efficiency. However, their use also presents risks that require clear policies and practices to ensure safety, security, and ethical application.

This acceptable use policy aims to ensure:

- Staff and volunteers are responsible users of AI and emerging technologies, prioritising safety and ethical considerations.
- School systems and users are protected from misuse or harm resulting from the use of AI.
- Staff have a clear understanding of their responsibilities when engaging with AI and emerging technologies in professional and personal contexts.

Acceptable Use Policy Agreement

I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of AI tools and technologies.
- I will only use AI tools and technologies for purposes authorized by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.
- I will ensure that any sensitive or personally identifiable information about staff, students, or parents/carers is only entered into AI systems that have explicit approval and robust security measures in place.
- I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

- I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.

- I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
- I will communicate professionally and responsibly when using AI systems.
- I will ensure transparency through appropriate attribution where AI has been used.

When engaging with learners:

- I will support learners on the safe, ethical, appropriate and effective use of AI.
- I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

- I will use AI systems in compliance with established security measures and access protocols.
- I will ensure that any AI applications used in teaching or administration are vetted and comply with the school's policies.
- I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

- I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.
- I will ensure I have explicit authorisation when uploading sensitive school-related information into generative AI systems.

Responsibility and Accountability:

- I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.
- I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.
- I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.

Agreement

I have read and understood the implications and my personal responsibilities in relation to the use of Artificial Intelligence

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name :
Role in School:
Signed
Date: