I

Online Safety and Acceptable Use Policy

Reviewed: 15.11.2023

Next Review: October 2024

Fairfields School

Inspiring everyone to shine

Approved by Governors 04.12.23

Fairfields School
Online Safety and Acceptable Use Policy

Introduction
At Fairfields we understand that Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Whilst exciting and beneficial to all in school, we need to be aware of the range of risks associated with the use of these technologies and want to ensure that all our pupils are safe when online and that clear expectations are in place for practices in school. This policy provides details of how systems and structures are set up in school and the responsibilities for staff and pupils when using technology.

Aims
Keeping Children Safe in Education, 2023 states
"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"

With Online Safety KCSIE identifies four key areas of risk

- **Content:** being exposed to illegal, inappropriate or harmful material;
- **Contact:** being subjected to harmful online interaction with other users;
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams

At Fairfields we aim:

- to ensure the safeguarding of all children within and beyond the school setting by detailing appropriate and acceptable use of all online technologies
- to outline the roles and responsibilities of everyone
- to ensure adults are clear about procedures for misuse of any online technologies both within and beyond the school setting
- to emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within, and outside of, the school environment
- to develop links with parents/carers to promote awareness of the benefits and potential issues related to technologies.

Legislation and Guidance
This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities
The governing board
The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

Approved by Governors 04.12.23

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The Designated Safeguarding Lead (DSL) takes **lead responsibility** for online safety as this falls within the area of safeguarding and child protection, Appendix A sets out the specifics of this part the role. At Fairfields the DSL is supported in leading this area by the Deputy DSL's, the Senior Leadership Team and the Scientific Technologies Learning Team.

The DSL's responisbilies in relation to online safety in school are in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

Approved by Governors 04.12.23

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

IT Management

As a school we commission Easi PC to manage our IT system. They are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the DSL or Deputy DSL as soon as possible.
- Following the correct procedures by informing the DSL/Deputy DSL if they need to bypass the filtering and monitoring systems for educational purposes, so these arrangements can be made with EasiPC.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy/child protection policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy/child protection policy
- Responding appropriately to all reports and concerns about cyber bulling, sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet, if developmentally appropriate

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International and Internet Matters

Approved by Governors 04.12.23

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating Pupils about Online Safety

Where relevant, based on pupils' understanding, we teach our children how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through Scientific Technologies and Physical, Health and Wellbeing, where concepts, skills and competencies have been taught by the time they leave in Year 6:

Appropriate skills and competencies are taught within the curriculum so that children have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Pupils will be taught about online safety as part of the curriculum:
All schools have to teach:

- Relationships education and health education in primary schools

Learning will relate to the developmental and cognitive ability of our pupils.
Pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

The teaching about safeguarding, including online safety, will be adapted in order to meet the individual needs of our pupils.

Educating parents about online safety

As a school we will raise parents' awareness of internet safety in letters or other forms of communications home, and in information via our website. This policy will also be shared with parents.
Online safety will also be covered during parents' evenings and annual review meetings where appropriate.
The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

The school will actively discuss cyber-bullying with pupils, where developmental appropriate, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE education, and other subjects where appropriate.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Approved by Governors 04.12.23

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Electronic Devices
As a school we understand that some of our pupils require electronic devices to help with regulation while on transport. If this is the case, the electronic device will be placed in the child's bag until the end of the school day.

In the event that a member of staff suspects that the content of the device poses a risk to staff or pupils, the Headteacher, and any member of staff authorised to do so by the Headteacher for example DSL and/or member of SLT, can carry out a search and confiscate any electronic device.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher/DSL
- If appropriate explain to the pupil why their device is being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation, if appropriate

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)
Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Approved by Governors 04.12.23

Fairfields recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.
Fairfields will treat any use of AI to bully pupils in line with our behaviour policy.
Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a dynamic risk assessment where new AI tools are being used by the school.

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

School systems
Network: - Our school network is set up on a cloud based server. This is run by Easi-PC through Amazon Web Services. All aspects of the Cloud are password protected with access rights, allowing staff to have access to areas required for their role in school. Each laptop and desktop is encrypted through Microsoft and runs Webroot Anti-Virus. Every member of staff has an individual login and password to the cloud network.

Internet :– Our current broadband provider is EXA Networks. We ensure we have safe and secure internet access through our robust internet content filtering provided through Securly Filter and the system is monitored through Securly Aware. Our WiFi is password protected with an Admin network for staff and a Guest network for all visitors to school.

Microsoft 365:- Microsoft 365 provides a secure cloudbased suite of apps to facilitate collaborative working and central location to house documents for staff to remotely access. Each member of staff has a password for the suite which ensures the content is secure.
Outlook: All staff have an email account which is password protected. If secure emails are needed to be sent to outside professionals which contain personal information these are sent using Egress Switch. Emails have an automated disclaimer which is designed to try and cover breaches of confidentiality, propagation of viruses, contractual claims and employee liability. Our disclaimer states:

> FAIRFIELDS DISCLAIMER: Any views or opinions expressed in this email and its attachments are solely those of the author and do not necessarily represent those of the company. The information in this e-mail message is confidential and may be legally privileged. It is intended solely for the addressee and access to this message by anyone else is unauthorised. If you have received the message in error, please notify us immediately and delete it. If you are not the intended recipient, any disclosure, copying, distribution or any other use is prohibited and may be unlawful. We accept no liability for damage related to data and/or documents which are communicated by e-mail.

It is important to manage e-mails to prevent personal data being dispersed. The guidelines set in Appendix B of this policy are intended to assist our staff to manage their e-mails in the most effective way.

- OneDrive: each member of staff has a OneDrive area to save their individual working documents.
- Teams: Microsoft teams is used by teams of staff within school for collaborative working. There is the facility to share documents, calendars and have a platform for team discussion.
- Sharepoint: Microsoft SharePoint is our secure central location for storing documents which are accessible by staff with the appropriate permissions. This is where all personal documentation is stored to meet the requirements of GDPR.

Approved by Governors 04.12.23

NB: Fairfields School has the infastructure for personal data to be stored securely across Microsoft 365. Documents which contain personal data will not be stored on memory sticks or portable harddrives.

To ensure that technology in school is clutter free and documents are easy to access Appendix C provides details on information management.

Portable Devices:- Across the school we use portable devices such as iPads to capture evidence of children's learning as a teaching and learning tool. These devices are password protected and apps are selected and checked by the class teacher. If apps need to be downloaded, these are approved by the Headteacher. This is also monitored by members of the safeguarding team.

Photos:- As part of our school activities, we take photographs and record images of individuals within our school. We obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
Some photos are required for us to carry out our role in school. We do not require consent for this as it fall unders the GDPR lawful basis criteria for fulfilling our public duty.

Evidence for Learning: We use the Evidence for Learning app to capture photos and videos as part of the system for recording children's learning. The app allows us to share the evidence collated with parents and colleagues connected to the pupils. The data and evidence collated is stored on the school's iPads and in cloud storage associated with the app. Only enabled and licenced devices have access to data stored. Data is transferred securely to the Cloud using industry-standard encryption technologies and protocols.The app has passcode protection which helps prevent unauthorised access. Each device is given a unique DeviceID and UserKey granting permissions to access only the school's data in the cloud. The Cloud Administrator has a password to maintain the system data stored in the Cloud. Cloud data is protected with class-level and object-level Access Control Lists. The Cloud service is hosted within the EU.

Social Media: At Fairfields we have Facebook, Instagram and 'X' social media accounts. This is so we can share our school profile, raise awareness of our setting and gain support from the local community. Posts include school activities, notices and events. Photos will only be used if we have sort consent from staff, visitors or parents. We also have a private facebook group as a school community page for our parents/carers. It is used for parents/carers to network with one another and school event details to be shared. Content is added and monitored by a member of the admin team and our family support worker.

GDPR – personal data and system security
We protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Personal Devices: Fairfields provides technology for staff to use to fulfil the requirements of their role in school. There is also adequate equipment for staff to use within school. On receipt of the hardware, a Laptop or iPad agreement is signed outlining the expectations of using the equipment. In the event that a member of staff needs to use their own equipment, they need to get permission from the Headteacher and ensure they follow the same security procedures as for school-owned equipment (For more information please see the Data Protection Policy).

Approved by Governors 04.12.23

Safety and responsibilities of staff (agreements and training)

All school based employees, including volunteers under the age of 18, must:

- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.
- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an online safety incident.
- report any Online Safety incident, concern or misuse of technology to a DSL, including the unacceptable behaviour of other members of the school community.
- use school computing systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of students. School issued email addresses, mobile phones and cameras must always be used by employees unless specific permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.
- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.
- not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.
- protect their passwords/personal logins and log-off or lock the network wherever possible when leaving work stations unattended.
- understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network.
- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.
- ensure that if personal devices are kept in school they are on silent and are stored in the classroom cupboard or in a staff locker and mustn't be used during directed teaching time.
- not use personal log ins to streaming services in school e.g. Netflix, Disney+, spotify
- consider the appropriateness of using video streaming sites e.g. youtube. If video clips are to be used to enhance learning, this are to be prewatched to monitor content and be embedded into powerpoints. Staff must ensure autoplay is disabled and will monitor the pop up adverts.

All staff are asked to sign a copy of the Acceptable Use Rules (Appendix D). A copy of these will be displayed in the staff room and Computer Room as a reminder that staff members need to safeguard against potential allegations.

In the event of inappropriate use

If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Allegations Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to managing concerns section of this policy for a list of actions relating to the scale of misuse.

Social Networking:- When using social media and instant messaging apps, staff need to ensure they are keeping their personal and professional lives separate. When comments are posted it must be made clear these are personal views and have not been made on behalf of the school. If a member of staff is unsure or concerned about the appropriateness of a post they should refrain from posting until it has been discussed with a member of the leadership team. All communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. Staff must not accept pupils' parent/carers as friends or use social media or instant messaging apps to send any personal messages to them directly or indirectly — personal communication could be considered inappropriate and unprofessional and may make staff vulnerable to allegations.

Approved by Governors 04.12.23

Staff may create groups on instant messaging sites in their class teams or as groups of colleagues to aid communication, networking and support. However, it is essential that they do not discuss wider school issues or pupils in this forum. Staff need to ensure that they are following our staff code of conduct when communicating in this manner.

NB: If staff carry out paid work for families, this needs to be disclosed to the Headteacher. In this situation the contact details can be stored on personal devices and social media can be used to communicate with the family, if done in a professional manner.

Pupils using mobile devices in school

As a school we understand that some of our pupils require electronic devices to help with regulation while on transport. If this is the case, the electronic device will be placed in the child's bag until the end of the school day. We have concerns about the use of mobile phones and have decided that their use is not allowed in school during directed teaching time.

Our concerns are:

- inappropriate or bullying text messages
- images or video taken of adults or peers without permission being sought

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device (This is included within the Microsoft 365 network)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.
Work devices must be used solely for work activities.
If staff have any concerns over the security of their device, they must inform the DSL/Deputy DSL who will seek advice from our IT Manager.

Safety and responsibilities of pupils (online safety in the curriculum)

Acceptable Use Rules and the letter for children and parents/carers are outlined in the Appendix E and detail how children are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any material. The rules are there for children to understand what is expected of their behaviour and attitude when using the Internet, which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

In the event of inappropriate use

Should a child be found to misuse the online facilities whilst at school the following consequences will occur:

- Access to the Internet will be suspended for a period of time and a letter will be sent home to parents/carers.
- A further letter will be sent where a child is deemed to have misused technology against another child or adult outlining the breach in the Child Protection Policy.

In the event that a child **accidentally** accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window.
Children should be taught and encouraged to consider the implications for misusing the Internet as this can lead to legal implications.

Approved by Governors 04.12.23

Managing a concern

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures below. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

A. An inappropriate website is accessed inadvertently:	B. An adult or child has communicated with a child or used ICT equipment inappropriately:	C. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

• Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
• Report website to the DSL if this is deemed necessary.
• Contact the helpdesk filtering service for school and LA so that it can be added to the banned list or use Local Control to alter within your setting.
• Check the filter level is at the appropriate level for staff use in school.
	• Ensure the child is reassured and remove them from the situation immediately.
	• Report to the Headteacher immediately.
	• Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
	• Contact CEOP (police) as necessary.
		• Preserve any evidence.
		• Inform the Headteacher immediately.
		• N.B. There are three incidences when you must report directly to the police.
		  ○ Indecent images of children found.
		  ○ Incidents of 'grooming' behaviour.
		  ○ The sending of obscene materials to a child.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

A. An inappropriate website is accessed inadvertently:	B. An inappropriate website is accessed deliberately or An adult has used ICT equipment inappropriately:	c. An adult has communicated with a child or used ICT equipment inappropriately:
• Report website to the DSL if this is deemed necessary. • Contact the filtering service for school and LA so that it can be added to the banned or restricted list. • Change Local Control filters to restrict locally. • Check the filter level is at the appropriate level for staff use in school.	• Ensure that no one else can access the material by shutting down. • Log the incident. • Report to the Headteacher and DSL immediately. • Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline. • Inform filtering services and the LA as with A.	• Ensure the child is reassured and remove them from the situation immediately, if necessary. • Report to the Headteacher and DSL immediately. • Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. • Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions. • If illegal or inappropriate misuse is known, contact the Headteacher or Chair of

		Governors (if allegation is made against the Headteacher) and Designated Safeguarding Lead immediately and follow the Allegations procedure and Child Protection Policy. • Contact CEOP (police) as necessary.

If an adult receives inappropriate material, they do not forward this material to anyone else – doing so could be an illegal activity. They need to alert the Headteacher immediately and ensure the device is removed and log the nature of the material. If needed the Headteacher will contact relevant authorities for further advice e.g. police.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted, this should be reported to the Headteacher.

Indecent images: CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine. Do not take a screenshot of the image. Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.
www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Training
All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

Working with Parents
Parents of pupils attending Fairfields School are made aware that they should only use personal devices to take photos of their own child and only post information about their own child on social media. We work with our

parents/carers, mainly on an individual basis, providing them with bespoke information about online safety and how to ensure their child is safe when using a device and is on the internet.

When a pupil is able to and needs more independent access to ICT and the internet within school, they will receive a copy of the Acceptable Use Rules (Appendix E). These rules need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules. It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted. School will keep a record of the signed forms.

Equal Opportunities
We value the views of all persons in our school community. The school acts in the best interests of the children, their parents / carers to encourage high quality provision that meets diverse needs and promotes equality.

Monitoring and Evaluation
The school will review this policy annually, in line with the review of the Child Protection policy, and its implementation and effectiveness will be assessed. The policy will be promoted and implemented throughout the school.

Links to other policies

- Data Protection
- Child Protection
- Health and Safety
- Quality of Education
- PSHE
- Behaviour
- Staff Code of Conduct

Approved by Governors 04.12.23

Appendix A
Role of the Online Safety Lead

Why should educational settings identify an online safety lead?

Online safety is an integral part of education settings' safeguarding responsibilities and requires strategic oversight and ownership to develop policies and procedures to protect all members of the community.

The online safety lead does not need to have vast technical knowledge, as it is a safeguarding and not a technical role. However it may be helpful if to have some basic knowledge of technology, as well as having an up-to-date understanding of the benefits and risks posed by the online environment.

Who should be the online safety lead?

'Keeping Children Safe in Education' (KCSIE) 2023 identifies online safety as a safeguarding concern. Additionally, Annex C recognises that responsibility for online safety falls within the remit of the Designated Safeguarding Lead (DSL). Some online safety incidents will reach thresholds for child protection action; therefore, the online safety lead should have a robust understanding of local safeguarding procedures. This means a DSL (or a suitably trained deputy DSL) will need to be involved in making any initial decisions regarding appropriate responses to online safety concerns. The online safety lead should also, where possible, be a member of the senior leadership team due to the strategic requirements and expectations of the role; for example, implementing policy, challenging practice and directing staff and resources.

What are the key tasks of the online safety lead?

Policies and Procedures

- Act as a named point of contact on online safety issues and liaise with other members of staff as appropriate.
- Ensure policies and procedures that incorporate online safety concerns are in place.
- Ensure there are robust reporting channels and signposting to internal, local and national support
- Record online safety incidents and actions taken, in accordance with the school's normal child protection mechanisms.
- Ensure the whole school community is aware of what is safe and appropriate online behaviour and understand the sanctions for misuse.
- Liaise with the local authority and other local and national bodies as appropriate.

Infrastructure and Technology

- Work with the leadership team and technical support staff, to ensure that appropriate filtering and monitoring is in place.
- Take appropriate action in line with child protection policies and procedures, if the filtering system and monitoring approaches identify any causes for concern.
- Work with the data protection officer to ensure that online practice is in line with current legislation.
- Work with the information security lead to ensure that online practice is in line with current legislation.

Education and Training

- Implement regular online safety training for all members of staff (including as part of induction) that is integrated, aligned and considered part of the overarching safeguarding approach (KCSIE 2021).
- Work with staff to ensure that appropriate online safety education is embedded throughout the curriculum; promoting the responsible use of technology and empowering children to keep themselves and others safe online.
- Actively engage with local and national events to promote positive online behaviour, e.g. Safer Internet Day and anti-bullying week.
- Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Ensure that their own knowledge and skills are refreshed at regular intervals to enable them to keep up-to-date with current research, legislation and trends.

Approved by Governors 04.12.23

Standards and Inspection

- Evaluate the delivery and impact of the setting's online safety policy and practice
- Review any reported online safety incidents to inform and improve future areas of teaching, training and policy development
- Feedback online safety issues to the management/leadership team and other agencies, where appropriate

Rebecca Avery, Education Safeguarding Advisor (Online Protection)
Ashley Assiter, Online Safety Development Officer
The Education People. November 2018

Approved by Governors 04.12.23

Appendix **B**
Good Practice for Managing E-mail

Introduction
The introduction of GDPR means that it is much more important to manage e-mail in schools to prevent personal data being dispersed around. These guidelines are intended to assist our staff to manage their e-mail in the most effective way, and should be used in conjunction with the existing policies on the use of ICT.

Things To Be Aware Of About E-mail

a) **E-mail has replaced telephone calls and memos**
As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written memo or a formal letter. E-mail should be laid out and formulated to our school's standards for written communications.

b) **E-mail is not always a secure medium to send confidential information**
We need to think about information security when we send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a civil penalty from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

c) **E-mail is disclosable under the access to information regimes**
All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything written in an email could potentially be made public.

d) **E-mail is not easy to delete permanently**
E-mails can remain in a system for a period of time after they have been deleted. Remember that although you may have deleted your copy of the e-mail, the recipients may not have and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998 and 2018.

e) **E-mail systems are commonly used to store information which should be stored somewhere else**
All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Creating and sending e-mail
We expect all staff to consider the following when sending e-mail.

Do I need to send this e-mail?
Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

To whom do I need to send this e-mail?
Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails. When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.

Is the subject of the email clear?
Having a clearly defined subject line helps the recipient to sort the e-mail on receipt. A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Approved by Governors 04.12.23

Is the e-mail clearly written?

- Do not use text language or informal language in school e-mails.
- Always sign off with a name (and contact details).
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
- Never write a whole e-mail in capital letters. This can be interpreted as shouting.
- Always spell check an e-mail before you send it.
- Do not use the urgent flag unless it is absolutely necessary; recipients will not respond to the urgent flag if they perceive that you use it routinely.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Do I need to send the attachments?

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Disclaimers

All emails sent from school will have a disclaimer added. This will help to mitigate risk, such as sending information to the wrong recipient, or to clarify the school's position in relation to the information being e-mailed. The disclaimer will cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school.

Filing e-mail

This school operates a Read, Act on, Delete policy regarding all emails that contain personal data. Email applications are not designed to store emails in a way in which their contents can be made securely available to other, appropriate, members of staff. If an email contains data which needs to be stored so that it can, if necessary, be shared then it will be dealt with as detailed below.

Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.

E-mail text and attachments

Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this and retain information which makes up the audit trail, is to save the e-mail in .msg format. This can be done either by clicking and dragging the e-mail into the appropriate folder in an application such as MS Outlook, or by using the "save as" function to save the e-mail in an electronic filing system. Emails can be saved and linked to a digital record in the MIS. If the e-mail needs to be re-sent it will automatically open into MS Outlook.

Where appropriate the e-mail and the attachments can be printed out to be stored on a paper file. However, a printout does not capture all the audit information which storing the e-mail in .msg format will.

E-mail text only

If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes. Alternatively the e-mail can be saved in .html or .txt format. This will save all the text in the e-mail and a limited amount of the audit information. The e-mail cannot be re-sent if it is saved in this format.

The technical details about how to undertake all of these functions are available in application Help functions.

How long to keep e-mails?

E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards.

Approved by Governors 04.12.23

E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule for schools found in the Records Management Tool Kit for Schools. These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

Approved by Governors 04.12.23

Appendix C
Information Management and Housekeeping Guidance

Housekeeping of Laptops/Desktops

To ensure all IT equipment runs smoothly and efficiently staff are asked to complete the following actions once a term

- Review their passwords, ensuring they are secure. It is advised that passwords are at least 8 characters long and include a capital letter, lower case letter, number and special character.
- Review their cloud storage and delete anything which is no longer needed or duplicates of items.
- Delete the emails in the deleted file on Outlook
- Review the emails in other files and delete any no longer needed.
- Empty the computer's recycle bin
- Delete the contents of the download folder

In addition to this a member of IT admin/IT technician will

- Check the users for the school system and delete any staff who have left.

Information Management Guidelines

When saving documents in shared areas the following rules will apply to ensure documents are easy to find and were last reviewed and updated:

Pupils' documents: pupils name, name of document, date

Jane Doe ILP 030519

Jane Doe Annual Review 170119

Staff Documents: staff name, name of document, date

John Smith Contract 191119

Other documents: Full Title of document, Date

Monitoring schedule 050619

Approved by Governors 04.12.23

Appendix D

Fairfields School
Inspiring everyone to shine

Online Safety Acceptable Use Rules for Staff and Volunteers

These rules apply to all on-line use, personal devices and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any online technologies, such as the Internet or email, they are asked to read these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of online technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must not use any personal devices or equipment for school related purposes
- I know that I should use the school equipment in an appropriate manner and for professional use.
- I know that images should not be inappropriate or reveal any personal information about children and that permissions must be acquired before uploading to the Internet.
- I have read the Procedures for Incidents of Misuse in the online safety policy so that I can deal effectively with any problems that may arise.
- I will report any accidental misuse.
- I will report any incidents of concern for the children's safety to the Designated Safeguarding Leads.
- I know who the Designated Safeguarding Leads in school are.
- I know it is not permitted and that I am putting myself at risk of misinterpretation and allegation should I contact children and/or parents via personal technologies, including my personal e-mail and social media
- I will inform the Headteacher of any out of school paid work that I do for parents of pupils who attend the school
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher.
- I know that I should complete virus checks on my laptop or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I keep my password secure and not disclose any security information, unless to appropriate personnel. If I feel someone inappropriate requests my password I will discuss this with one of the Designated Safeguarding Leads.
- I have access to a copy of the Online Safety Policy to refer to about all online safety issues and procedures that I should follow.
- I will adhere to copyright guidelines.
- When using social media and instant messaging apps I will ensure I make clear these are personal views and have not been made on behalf of the school. I will ensure I do not make comments directly linked to school or pupils
- When using instant messaging sites e.g. whatsapp, particularly in groups I will not discuss sensitive school matters, share school related documents or discuss pupils.
- I will not use personal log ins to streaming services in school e.g. Netflix, Disney+, spotify
- I will consider the appropriateness of using video streaming sites e.g. youtube. If video clips are to be used to enhance learning, I will make sure these have been prewatched to monitor content and will be embedded into powerpoints. I will ensure autoplay is disabled and will monitor the pop up adverts.
-

Name …… Signed…….. Date……..

Approved by Governors 04.12.23

Fairfields School
Inspiring everyone to shine

Online Safety Acceptable Use Rules Letter to Parents/Carers

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet via the school's designated Broadband supplier.

In order to support the school in educating your child about Online Safety (safe use of the Internet), please read the following Rules with your child then sign and return the slip.

In the event of a breach of the Rules by any child the Online Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact either me or the Online Safety Leader (Mrs Sara Clarkson) at school.

Yours sincerely,

Mrs Lesley Elder
Headteacher

.....

Online Safety Acceptable Use Rules Return Slip

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the Internet, E-mail and online tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other online tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

Approved by Governors 04.12.23

Appendix E

Fairfields School
Inspiring everyone to shine

These are our rules for using the Internet safely and responsibly.

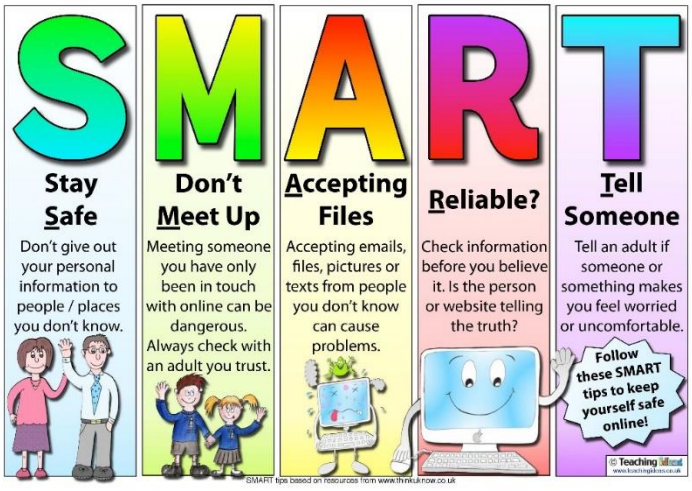
Key Stage 2

Our Online Rules

The school has installed computers with internet access to help our learning. These rules will help keep us safe and help us be fair to others.

- We use the Internet to help us learn and we will learn how to use the Internet safely and responsibly.
- Adults are aware when we use online tools.
- We never give out passwords or personal information (like our surname, address or phone number).
- If we need help we know who to ask.
- If we see anything on the Internet or in an e-mail that makes us uncomfortable, we know what to do.
- If we receive a message sent by someone we don't know we know what to do.
- We know we should follow the rules as part of the agreement with our parent/carer.
- We are able to look after each other by using our safe Internet in a responsible way.

Remember to be SMART:



Approved by Governors 04.12.23

Fairfields School
Online Safety and Acceptable Use Policy - Remote Learning

Virtual communication

Teachers should think about:

- Ensure you are fully prepared for the call considering all of the below before you start as well as any resources you would like to use.
- The teacher should remain on the call at all times to ensure that appropriate behaviour and communication is maintained between all people involved.
- When setting up a meeting ensure it has a lobby so you are in control of who is in the call. Instructions for this can be found on SharePoint.
- Ensure that parents are informed in good time of when calls are going to happen and ensure that this is within school hours.
- At all times consider the challenges our pupils parents are under and be flexible explaining calls are to support their children and their learning but if they are not suitable or do not work for them they are not compulsory.
- Dress appropriately as you would in school
- Ask all parents / pupils to ensure that they maintain boundaries and appropriate behaviour (good listening, looking etc.)
- Think about where you are conducting the call and if necessary use signs to indicate 'Call in progress/do not disturb' to ensure no unplanned interruptions. Calls via teams, video or audio, can be conducted from home. Telephone calls must take place on school telephones. It is the parents choice how they are communicated, if they want a telephone call it will have to be from a teacher who is in school between 3-3:45.
- If you feel you are on your own on the call with a child you should check that a parent is still nearby – you should not be on a call on your own with a child – if this is the case you must end the call immediately.
- If you feel anything inappropriate is happening you are able to click people out of the call and should do this instantly and follow up to explain.
- If you become aware the children and parents are in a bedroom or personal space you will need to ask them to move to another more communal area
- If you plan to share your screen ensure you only allow what is required to be seen. Prepare your desktop before the call to ensure this is also appropriate with internet tabs and documents.
- Teachers should be the last one to leave the call – indicating to parents that you are waiting for everyone to leave
- After your call immediately add to call logs on SharePoint and inform Key Stage leader of any concerns via email.
- Report concerns with any remote learning calls regarding online safety or safeguarding issues on MyConcern and to a member of the DSL team.

By accepting the link to a **Class video call** parents are agreeing to:

- Not take screen shots or pictures of any children on screen and only immediate family and carers will have access to the call
- Ensure that your device is muted until asked by Class Teacher to turn microphones at different times in the call.
- Ensure you are in a safe space for the call to take place and consider your surroundings. We ask that you are not in bedrooms.
- Ensure that you are around to be in control of the device used and remain in earshot of the device whilst your child is on the call
- An understanding that you and your child will be on a group call with the class teacher, support staff where possible, and other pupils and their parents.
- Ensure that nothing is shared that other parents may not want their children to see
- If a teacher feels inappropriate behaviour, language or visuals (paintings, ornaments etc.) are displayed they will remove individuals from the call / end the call and contact to explain.

Approved by Governors 04.12.23

- Understanding you have the ability to report concerns to the school office and ask to speak to a Designated Safeguarding Lead if you have any concerns with anything shared on the call.
- Online safety support for parents at home has been added to our home learning sections

Approved by Governors 04.12.23