Lacey Green Primary Academy
Online Safety Policy

Policy Reviewed and Agreed at Full Governing Body Level: November 2025

This policy includes the following appendices:

- Computer and Internet Acceptable Use Guidelines for staff, pupils and visitors
- Mobile Phone Use Policy

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** - being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, violence, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** - being subjected to harmful online interaction with other users, such as child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Legislation and Guidance

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

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying: advice for principal and school staff.
- Relationships and sex education.

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. It also reflects the Education Act 2011, which gave 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 Body

The Governing Body has overall responsibility for monitoring this policy and holding the Principal to account for its implementation. The Governing Body 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 Body will also ensure all staff receive regular online safety updates as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Body will:

- Co-ordinate regular meetings with appropriate staff to discuss online safety.
- Ensure children are taught how to keep themselves and others safe, including keeping safe online.
- 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.

The **Trustee** who oversees online safety is Karen Bailey.

All **Trustees** will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 1).
- 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).

The Principal

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

The Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety. However, at Lacey Green Primary Academy, the Head of School who is also trained as a DSL, assumes operational responsibility for online safety. Details of the school's designated safeguarding lead and deputies are set out in our child protection and safeguarding policy.

In particular, the Head of School takes operational responsibility for:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Principal and Governing Body 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 IT manager to make sure the appropriate systems and processes are in place.
- Working with the Principal, IT 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 relevant online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy.
- 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 Principal and/or Governing Body.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Working alongside the DSL to provide 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.

The IT manager

JTRS manage the IT systems at **Lacey Green Primary Academy**. 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. At Lacey Green Primary Academy we use **Securly.**
- Ensuring that the school's IT 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 IT 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 shared with the online safety lead / DSL.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

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 IT systems and the internet (appendix 1) and ensuring that pupils follow the school's terms on acceptable use (appendices 2 and 3).
- Knowing that the Head of School (Deputy 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 Head of School and IT Manager.
- Following the correct procedures by consulting the Head of School if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the Head of School/DSL to ensure that any online safety incidents are logged on CPOMs 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.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy.

Parents/carers 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.

Visitors and members of the community

Visitors and members of the community who use the school's IT 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 (appendix 1).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. This will be covered through the school's computing, Personal Development and RSE curriculums.

In **Key Stage 1**, 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.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, Victims of abuse and some pupils with SEND.

Educating parents about online safety

The school will raise parents' awareness of online safety through ClassDojo updates, especially as incidents arise. Parental curriculum overviews are shared each half term with all parents.

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 one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the Victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The school's computing and PSHE curriculums set out what children will learn about cyber-bullying.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. For new staff, this is completed as part of their school induction.

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. 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.

Examining electronic devices

The senior leadership team (SLT) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the member of SLT 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 Principal / DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation.
- Contact parents/carers where appropriate.

The school's leadership team 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 SLT 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 school's 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 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 a member of the safeguarding team) 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.
- The school behaviour policy.

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 (Al)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Lacey Green Primary Academy recognises that Al 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 Al is used to create images, audio or video hoaxes that look real. Lacey Green Primary Academy will treat any use of Al to harm pupils in line with our anti-bullying and behaviour policies. Staff should be aware of the risks of using Al tools whilst they are still being developed and should carry out a risk assessment where new Al tools are being used by the school.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 to 3). 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, trustees and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices 1 to 3.

Pupils using mobile phones in school

Pupils in Year 5 and 6 may bring mobile phones into school but are not permitted to use them during the school day. They are handed in at the start of the school day and collected once school has finished. During the day, they are kept in the school office.

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.
- Making sure the device locks if left inactive or unattended for a period of time.
- Not sharing the device among family or friends.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from JTRS.

How the school will respond to issues of misuse

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

Where a staff member misuses the school's IT 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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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, and CPD sessions).

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, deputy DSLs and members of the school's safeguarding team 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.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training via the National College. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

Behaviour and safeguarding issues related to online safety are logged by school staff on CPOMs. This policy will be reviewed every 2 years or in line with new national guidance by the Head of School. At every review, the policy will be shared with the Governing Body.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy.
- Behaviour and Anti Bullying policy.
- Staff disciplinary procedures.
- Data protection policy and privacy notices.
- Complaints procedure.
- IT and internet acceptable use policy.
- Tracker and Smartwatch Policy

Appendix 1: Computer Acceptable Use – Staff Guidelines

The staff at **Lacey Green Primary Academy** has been provided with computers to aid the planning, organisation and delivery of subjects across the entire curriculum. The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all.

Equipment

- Always get permission from JTRS / Head of School before installing, attempting to install or storing programs of any type on the computers.
- Please take care of computers. Damaging, disabling, or otherwise harming the operation of computers, puts your work at risk.
- You are welcome to take your laptop off the school premises to use for school purposes.
- All files should be saved to the Google Drive – No external devices to be used on the network.
- Protect the computers from spillages by eating or drinking well away from the IT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or photograph to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Always update school software when prompted.

Internet

- You should access the Internet sensibly and appropriately.
- Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.

Email

- Be polite and appreciate that other users might have different views from your own.
- Always consider the sender when opening attachments to emails if they don't come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of SLT. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

Appendix 2: Computing Acceptable Use - Agreement for KS1 Pupils

Covered as part of the Computing and Personal Development Curriculum.

When I use the school's IT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them.
- Only use websites that a teacher or adult has told me or allowed me to use.
- Tell my teacher immediately if:
    - I click on a website by mistake.
    - I receive messages from people I don't know.
    - I find anything that may upset or harm me or my friends.
- Use school computers for school work only.
- Be kind to others and not upset or be rude to them.
- Look after the school IT equipment and tell a teacher straight away if something is broken or not working properly.
- Only use the username and password I have been given.
- Try my hardest to remember my username and password.
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.
- Save my work on the school network.
- Check with my teacher before I print anything.
- Log off or shut down a computer when I have finished using it.

Appendix 3: Computing Acceptable Use - Agreement for KS2 Pupils

Covered as part of the Computing and Personal Development Curriculum.

I will read and follow the rules in the acceptable use agreement guidelines.

When I use the school's IT systems (like computers) and get onto the internet in school I will:

- Always use the school's IT systems and the internet responsibly and for educational purposes only.
- Only use them when a teacher is present, or with a teacher's permission.
- Keep my usernames and passwords safe and not share these with others.
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer.
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others.
- Always log off or shut down a computer when I've finished working on it.

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including in emails.
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate.
- Log in to the school's network using someone else's details.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

If I bring a personal mobile phone into school:

- I will only bring a mobile phone to school if I am in year 5 or 6.
- I will hand my mobile phone to the school office for it to be stored away safely during the school day.
- If I bring another device to school for medical reasons, this will only be used for medical purposes and under the supervision of an adult.

Appendix 4: Mobile Phone Policy

Relevant guidance

This policy meets the requirements of the Department for Education's non-statutory mobile phone guidance and behaviour guidance. Further guidance that should be considered alongside this policy is Keeping Children Safe in Education.

Roles and responsibilities

Staff

All staff (including teachers, support staff and supply staff) are responsible for consistently enforcing this policy.

Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.

The Head of School is responsible for monitoring the policy every 2 years, reviewing it, and holding staff and children accountable for its implementation.

Staff will address any questions or concerns from parents/carers quickly, and clearly communicate the reasons for prohibiting the use of mobile phones.

Use of mobile phones by staff

The DfE's non-statutory mobile phone guidance says that staff should not use their own mobile phone for personal reasons in front of pupils throughout the school day.

Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone, while children are present. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time for personal reasons. For instance (this list is non-exhaustive):

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The Head of School will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number 01625 525157 as a point of emergency contact.

Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Gemini).

Safeguarding

Staff must not give their personal contact details to parents/carers or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents/carers or pupils.

Staff must not use their personal mobile phones to take photographs or recordings of pupils, their work, or anything else that could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

If your school uses classroom apps or programmes that require the use of a member of staff's mobile phone, you should explain the appropriate use of mobile phones in these circumstances.

Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but are not limited to:

- Use of multi-factor authentication
- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else that could identify a pupil

Work phones

Some members of staff are provided with a mobile phone by the school for work purposes.

Only authorised staff are permitted to use school phones, and access to the phone must not be provided to anyone without authorisation.

Staff must:

- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct

Sanctions

Staff members who fail to adhere to this policy may face disciplinary action.

See the school's staff disciplinary policy for more information.

Use of mobile phones by parents/carers, volunteers and visitors

Parents/carers, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not using mobile phones anywhere on the school site or on school trips.
- Not taking pictures or recordings of pupils, unless it's at a public event (such as a school fair / school performance), or of their own child
- Using any photographs or recordings for personal use only, and not posting on social media without consent

- Not using phones in lessons, or when working with pupils

Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents/carers or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents/carers
- Take photos or recordings of pupils, their work, or anything else that could identify a pupil

Loss, theft or damage

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or while pupils are travelling to and from school.