# Online Safety Policy

# September 2026

**This is a Statutory Policy**

**This policy was adopted in September 2025 and in consultation with staff and Governors and reviewed in September 2026.**

**It was ratified by the Board of Governors on_____**

**REVIEW: This policy will be reviewed annually (next review September 2027)**

**APPROVAL: Headteacher & staff plus governors**

**AGREED:**

**Chair of governors: _____**

**Headteacher: _____**

| | |
|---|---|
| Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring | Alison Grigg |
| Deputy Designated Safeguarding Leads / DSL Team Members | Hannah Hunt and Sarah Martin |
| Link governor for safeguarding (including webfiltering) | Peter Vardon |
| Curriculum leads with relevance to online safeguarding and their role | Sophie Besant<br>Alison Grigg |
| Network manager / other technical support | Laurence Francis DLSolutions |
| Date this policy was reviewed and by whom | September 2026 staff and Governing Board |
| Date of next review and by whom | September 2027 staff and Governing Board |

## Overview

### Aims

This policy aims to:

- Set out expectations for all Broomgrove Infant School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

## Scope

This policy applies to all members of the Broomgrove Infant School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

## Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

## Board of Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents, monitoring reports and reviewing protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards. Peter Vardon has taken on the role of Safeguarding Governor and this includes Online Safety. As part of this role, Peter Vardon works closely with the DSL on the new filtering and monitoring standards. Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any group involved in technology / online safety / health and safety / child protection. Governors should take part in training sessions that may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association or other relevant organisations
- Participation in school training/information sessions for staff or parents (this may include attendance in assemblies/lessons).

## Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing/Online Safety Subject Lead.
- The headteacher ensures that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised

- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per DfE standards—through regular liaison with technical colleagues– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- This will involve starting regular checks and annual reviews, upskilling the DSL and working with filtering and monitoring governor
- The Headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (Appendix 1 – ICT Acceptable Use Policy Code of Conduct and Appendix a flow chart in the Disciplinary Procedure Policy).
- The Headteacher reviews protections for remote-learning procedures, rules and safeguards
- The Headteacher is responsible for ensuring that other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- The Headteacher ensures that policies and procedures are followed by all staff
- The headteacher ensures governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

### Computing/Online safety Subject Lead

The Computing/Online Safety Lead is responsible for:
As listed in the 'all staff' section, plus:

- Day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensure "An effective whole school approach to online safety" as per KCSIE
- Responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Overseeing the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Ensuring that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Working closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Working closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

- Collaborating with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff
- Overseeing the protections for remote-learning procedures, rules and safeguards
- Meeting regularly with Safeguarding/Online Safety Governor to discuss current issues and review incident logs

### Network Manager (DLSolutions)

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE).
- That the school meets required online safety technical requirements and any Essex County Council Online Safety Policy or Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are individual to each user.
- The Essex County Council filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
  That the use of the network, internet, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Computing/Online Safety Subject Lead for investigation/action/sanction.

### Designated/Deputy Safeguarding Lead

The DSL is responsible for:

- The DSL should "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- Ensure "An effective whole school approach to online safety" as per KCSIE
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- Responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the filtering governor to learn more about this area, better understand, review

and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home

- Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Receiving regular updates in online safety issues and legislation, be aware of local and school trends
- Promoting an awareness of and commitment to online safety throughout the school community

The DSL should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Filtering and Monitoring
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

### Teachers

- Teachers and Support Staff are responsible for ensuring that:
- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- Be aware of the DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.
- They have read and understood Staff Code of Conduct and follow the acceptable use policy
- All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems
- Online -safety awareness are embedded in all aspects of the curriculum and other activities including for homework and remote learning
- They know that RSHE is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- They understand that online safety is a core part of safeguarding; as such it is part of everyone's job
- They record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures to the Headteacher or Computing/Online safety Subject Lead
- When they support pupils remotely, they are aware of additional safeguarding considerations and promote safe behaviours

- They prepare and check all online source and resources before using and follow processes for dealing with any unsuitable material that is found in internet searches
- They take a zero-tolerance approach to bullying and sexual harassment
- They model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

### Pupils

Pupils need to:

- Treat **home learning** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

### Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. They should:

- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away

from beds/bedding/personal information etc. and the background blurred or changed where possible.

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns

## Education

We follow Project Evolve to ensure fair coverage of the key strands from the Connected World document and that these are age appropriate and in addition to the CEOP unit on online safety
The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.
Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
At Broomgrove Infant School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety). We follow Project Evolve to ensure an age appropriate coverage of the key strands from the Connected World document, in addition to the CEOP unit on online safety

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

### Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the Computing/Online Safety Subject lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Child Protection Policy
- Harmful Sexual Behaviour Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the Computing/Online Safety Subject Lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

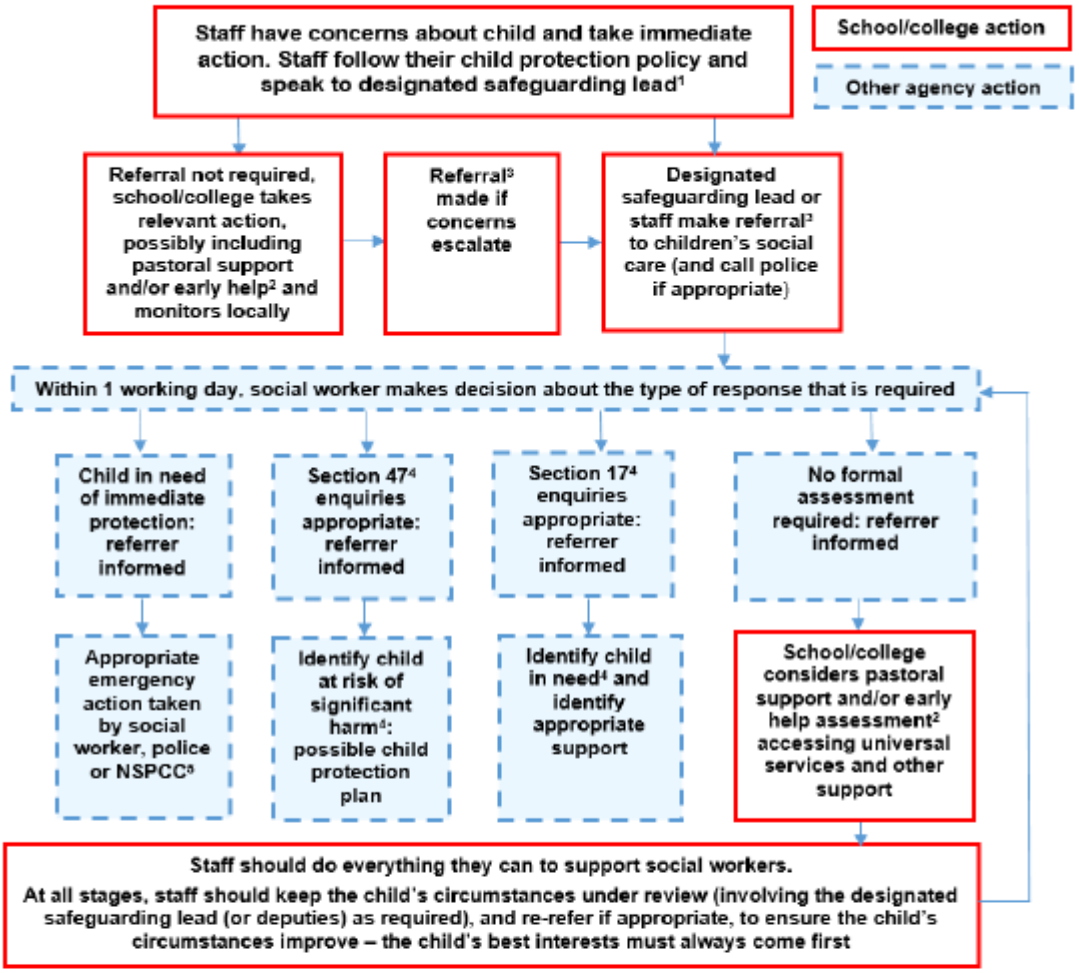
Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2026 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

**Figure 1: Flowchart setting out the actions taken where there are concerns about a child**




[1] In cases which also involve a concern or an allegation of abuse against a staff member, see Part four of this guidance.

[2] Family Help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated Family Help, a family help inter-agency assessment should be arranged. Working Together to Safeguard Children provides detailed guidance on the Family Help process.

[3] Referrals should follow the process set out in the local threshold document and local protocol for assessment. See Working Together to Safeguard Children.

[4] Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Working Together to Safeguard Children.

[5] This could include applying for an Emergency Protection Order (EPO).

### Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. See Anti-bullying Policy.

### Appropriate filtering and monitoring

Staff are aware of the changes and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. Staff can submit concerns at any point via email to the headteacher/DSL and will be asked for feedback at the time of the regular checks which will now take place half termly.
At Broomgrove Infant School:

- web filtering is provided by Webscreen by LGFL on school site
- changes can be made by Alison Grigg, Daniel Bennett and DLSolutions
- overall responsibility is held by the DSL
- technical support and advice, setup and configuration are from Mark Lester DLSolutions
- regular checks are made half termly by DSL to ensure filtering is still active and functioning everywhere. These are evidenced through log and report checking.
- an annual review is carried out as part of the online safety audit to ensure a whole school approach
- guidance on how the system is 'appropriate' is available at appropriate.lgfl.net

At Broomgrove Infant School, we use a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

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

### Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For school website
- For social media

- For local newspapers

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.
Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).
All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Broomgrove Infant School, no member of staff will ever use their personal phone to capture photos or videos of pupils.
Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.
Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).
Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children
Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

### Data protection and data security

All pupils, staff, governors, volunteers and parents are bound by the school's data protection policy and agreements, which can be found on the school website
The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.
Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.
"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care,

and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children**."

### Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages. When using communication technologies the school considers the following as good practice:

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

### Social Media

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. We manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

We expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.
This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.
If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).
Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), however the school deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.
However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.
Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).
Email is the official electronic communication channel between parents and the school. Communication with parents and pupils will also take place through Tapestry and Microsoft Teams, particularly when using these platforms to deliver remote learning.
Pupils are not allowed to be 'friends' with or make a friend request to any staff, governors, volunteers or otherwise communicate via social media.
Pupils are discouraged from 'following' staff, governor, or volunteer public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.