Digital Technology & Online Wellbeing Policy

Riccall Community Primary School

This policy was reviewed by the school on:	25th March 2026
Estimated next review date	March 2026

Contents:

1. Aims
2. Legal framework and guidance
3. Roles and responsibilities
4. Class use of technology
5. Internet access
6. Network security
7. The school website
8. Use of school devices
9. Digital and video images
10. Emails
11. Social networking
12. Filtering and monitoring systems
13. Remote learning
14. Educating pupils about online safety
15. Educating parents about online safety
16. Cyber-bullying
17. Acceptable use of the internet in school
18. Pupils using mobile devices in school
19. Staff using work devices outside school
20. How the school will respond to issues of misuse
21. Training
22. Monitoring arrangements
23. Links with other policies

Appendix A Online safety incident Flow chart
Appendix B acceptable use policies

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- 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 devices)
- 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, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer 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., consensual and non-consensual sharing of nudes and semi nudes and/or pornography), sharing other explicit images and online bullying; and
- **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, and its advice for schools on:

- Teaching online safety in schools
- Preventing-and-tackling-bullying and Cyber bullying: advice for headteachers and school staff
- Relationships and sex-education
- Searching-screening-and-confiscation
- Protecting children from radicalisation
- Mobile phones in schools

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the https://www.legislation.gov.uk/ukpga/1996/56/contents (as amended), the Education and Inspection 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

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the Designated Safeguarding Lead and the Headteacher who will receive regular information about online safety incidents and monitoring reports.

A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead regularly receiving (collated and anonymised) reports of online safety incidents.
- checking that provision outlined in the Online Safety Policy (e.g., online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant governors group/meeting
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- membership of the school Online Safety Group The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

The headteacher

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the dayto-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead .
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

The designated safeguarding lead.

The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)

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 DSL is responsible for:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- 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 child protection policy
- Ensuring 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 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 and filter and monitoring reports to the headteacher and/or governing board.
- The DSL is responsible for overseeing the DfE Digital and technology standards in Schools (filtering and monitoring) standards, including:
    - Receiving and reviewing filtering and monitoring reports
    - Responding to filtering and monitoring alerts and addressing safeguarding concerns
    - Completing checks to filtering and monitoring systems
    - Raise staff awareness to the school staff and pupils.

IT Provider and IT Technician – Riccall Primary School's IT provision is provided by Vital and monitored by Caroline Adams and the Designated Safeguarding Lead.

The Provider is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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.
- Internal system has an anti-virus to alert of any breaches in security.

The Designated Safeguarding Lead is responsible for:

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous file
- Overseeing the filtering and monitoring system in line with Digital and technology standards in Schools, including:
    - maintaining filtering and monitoring systems
    - providing filtering and monitoring reports
    - completing actions following concerns or checks to the system.

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.
- Working with the DSL to ensure 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.
- 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'.

Pupils

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed).
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies in and out of school.

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.

Parents can seek further guidance on keeping children safe online by information provided on the school website, online safety section.

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.

Classroom use of technology

A wide range of technology is used during lessons, including the following:

- **Laptops**
- **Tablets**

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by **Vital.** Smoothwall is always turned on.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.

All staff and governors will complete cyber security training.

Staff members and pupils

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils have their own individual Wonde log-in that they must not share.

Staff members are responsible for keeping their passwords private and 2 factor authentication is also used for staff and governor accounts when used off-site.

Users are required to lock access to devices and systems when they are not in use.

Users inform ICT technicians if they forget their login details, who will arrange for the user to have their username and password to be reset.

Our server is backed up on Redstor in case of malicious attacks.

The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if the provisions in the Photography Policy are met.

Use of school-owned devices

Staff members are issued with the following devices to assist with their work:

- iPad
- Laptop

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g., tablets to use during lessons.

School-owned devices are used in accordance with the Device User Agreement.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

All school-owned devices are password protected.

No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

Any cyberattacks initiated through emails are managed in line with the Information Security Incident Reporting Policy.

Social networking

Personal use

Access to social networking sites is filtered as appropriate.

Staff are not permitted to use social media for personal use during lesson time.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. Please see the school code of conduct for further details.

Staff receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. (Staff to refer to the school code of conduct)

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g., Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Social networking use on behalf of the school.

The use of social media on behalf of the school is conducted in line with the Acceptable Use Policy.

The school's official social media channels are only used for official educational or engagement purposes.

Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The following must be adhered to by all staff, volunteer and visitors:

- staff/volunteers must be aware of those pupils whose images must not be taken/published. **Those images should only be taken on school devices.** The personal devices of staff should not be used for such purposes.
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- care should be taken when sharing digital/video images that pupils are appropriately dressed.
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy.
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media.
- permission is not required for images taken solely for internal purposes.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- mages will be securely stored in line with the school retention policy.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act).

To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Filtering and monitoring online activity.

The governing body ensures the school's ICT network has appropriate filters and monitoring systems in place. Riccall Primary school, use Smoothwall filtering and monitoring systems.

The headteacher and IT technicians undertake a risk assessment to determine what filtering and monitoring systems are required.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The governing body ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

IT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the Headteacher.

Prior to making any changes to the filtering system, IT technicians and the DSL conduct a risk assessment.

Any changes made to the system are recorded by IT technicians.

Reports of inappropriate websites or materials are made to the **IT technician and DSL** immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and IT technicians, who will escalate the matter appropriately.

If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g., the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored.

All users of the network and school-owned devices are informed about how and why they are monitored.

Concerns identified through monitoring are reported to the DSL who manages the situation in line with the schools safeguarding policy and behaviour policy.

Remote learning

All remote learning is delivered in line with the school's Pupil Remote Learning Policy.

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.

- Use appropriate language – this includes others in their household.

Maintain the standard of behaviour expected in school.

- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g., to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.

Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will consult with parents at least two weeks prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g., ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g., sites they have been asked to use and staff they will interact with.

- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g., anti-virus software, on devices not owned by the school.

Educating pupils about online safety

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

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 internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. The school shares details of online safety information presentations via the school newsletter.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filtering 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

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. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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.

Artificial intelligence (AI)

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 Bard. Riccall Primary School 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.

Riccall Primary School will treat any use of AI to bully pupils in line with our Anti-Bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used and gain approval from the headteacher. Please see the school's Generative AI policy for further information.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to agree to 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.

Using mobile devices in school

Staff & Governors

As stated in the staff code of conduct, the school accepts that employees will bring their own devices into the workplace and may use them for work purposes e.g. sending and receiving work e-mails on a mobile phone or tablet, or wearing a smartwatch. When employees are using personal devices for work purposes, including accessing guest Wi-Fi whilst on school premises, then the standards contained in this Code will apply to their use and usage will be monitored.

The personal use of mobile phones during working hours should be undertaken with discretion. Employees should not make or receive calls or texts during work time where pupils are present. Mobile phones should be on silent at all times whilst in school and should not be left on display, with the exception of places determined by the school.

Employees are not permitted to use their personal devices for making voice or video recordings within school or taking photos of pupils. If there is a requirement in the individual's role to take photographs of children for school purposes, this should be carried out using school equipment which will be provided with the agreement of the Headteacher/senior manager and in line with the agreed school procedures and where appropriate permissions have been sought.

All staff should consistently enforce the school's policy on the use of mobile phones.

Visitors to the school

The following information is shared with visitors to the school when they sign-in:

The use of personal mobile phones or other devices capable of recording audio or visual information is not permitted by visitors without permission given by the Headteacher or other appropriate member of staff.

Use of the school's internet network is 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 on the school network to ensure that they comply.

We do not consent to any recording (either audio or visual) of any pupils, staff members or other visitors on site without permission given by the Headteacher or other appropriate member of staff.

Pupils

Pupils may bring mobile phones into school to support medical needs or emergency use only, with agreement from the Headteacher but are not permitted to use them for any other purpose during:

- The school day
- Clubs before or after school, or any other activities organised by the school, or at discos and events organised by Friends of Riccall School.

Mobile devices, including phones, should not be taken on any school trip.

A watch that counts steps such as a fitbit is fine, however, any device that is able to send/receive calls and messages or take photographs is treated the same as mobile phones and should not be used during the school day or any other activities organised by the school..

If a pupil carries a mobile device to school, this must be handed to the class teacher at the beginning of the day. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Where pupils and staff need access to their mobile device to monitor health needs during the school day will be agreed by the headteacher as part of their medical support plan.

Any breach of the acceptable use agreement by a pupil may trigger sanctions action in line with the school behaviour policy, which may result in the confiscation of their device.

Parents

Parents are asked to support the school's policy on mobile devices by helping ensure that pupils do not bring their phone into school and if they do, they follow the guidelines set out above, particularly with ensuring that devices are handed in at the start of the day at that they are not taken on school trips.

Where parents need to contact their child during the school day, they should contact the school office and the message to the pupil will be passed on from there.

Parents are also asked to not use airtags or smart tags other tracking devices to monitor the location of pupils on visits as this can alert staff and other members of the public that they are

being followed and can cause unnecessary panic or disruption amongst students and the public.

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)
- 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 which 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 seek advice from the IT Technician.

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 our policies on behaviour and internet acceptable use. All incidents must be reported to the DSL.

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 must be reported to the headteacher and 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Examining electronic devices

The headteacher and any member of staff authorised to do so by the headteacher (as set out in your behaviour policy), 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 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 or DSLs.
- 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.

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 headteacher or DSL 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 equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on Searching, screening and confiscation and the 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
- School's 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.

If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart] appendix A), the incident must be escalated through the agreed school safeguarding procedures, this may include:

- Non-consensual images
- Self-generated images
- Terrorism/extremism
- Hate crime/ Abuse
- Fraud and extortion o Harassment/stalking
- Child Sexual Abuse Material (CSAM) or Child Sexual Exploitation Grooming
- Extreme Pornography
- Sale of illegal materials/substances
- Cyber or hacking offences under the Computer Misuse Act
- Copyright theft or piracy

Training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated regularly and is delivered in line with advice from the three local safeguarding partners.

In addition to this training, staff also receive regular online safety updates as required and at least annually.

The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

All staff are informed about how to report online safety concerns. The DSL acts as the first point of contact for staff requiring advice about online safety.

Monitoring arrangements

The DSL monitors all logs of behaviour and safeguarding issues related to online safety on CPOMs. Staff incidents should be reported immediately to headteacher.

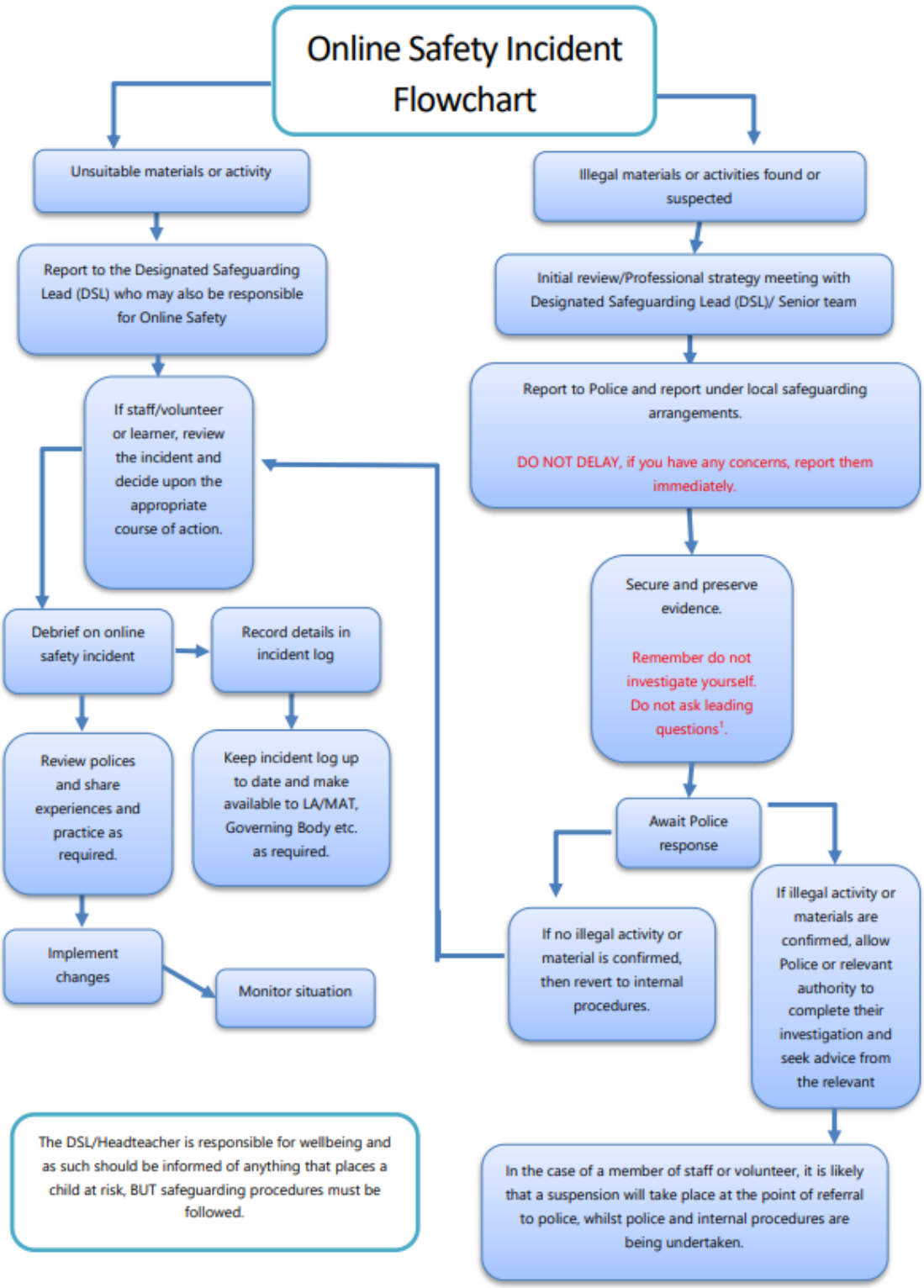
This policy will be reviewed every year. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy
- Workforce privacy notice
- Governors and volunteer privacy notice
- Website privacy notice
- Information security policy, including Acceptable Use Policies
- Complaints procedure
- Generative AI policy

Appendix A


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes
Monitor situation
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
Illegal materials or activities found or suspected
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Appendix 2: Workforce Acceptable Use Policy (Adapted from Veritau Information Security Policy)

The document governs our workforce's use of the corporate network and cloud-based systems, including when authorised to use personal devices.

Email, Instant Messaging, and Internet Use

We provide the workforce with email accounts, instant messaging (IM) functionality, and Internet access to assist with performing their duties. For the benefit of doubt, Instant Messages are classed as email communications in this policy.

Personal use
Whilst email accounts, IM, and the Internet should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Use must not tarnish our reputation or infringe on business functions
- Emails sent to and from corporate accounts are our property
- We may monitor the use of accounts and systems and access any personal messages and browsing history contained within
- Emails sent to or from their email account may be disclosed under Freedom of Information and/or Data Protection Legislation
- We reserve the right to cleanse email accounts at regular intervals, which could result in personal emails being erased from the corporate network
- We reserve the right to suspend access to accounts and systems anytime.

Inappropriate use
We do not permit users to send, forward, or solicit emails, or use the Internet in any way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic messages, images, cartoons, jokes, or movie files
- Unwelcome propositions, profanity, obscenity, slander, or libel
- Any messages or content containing ethnic, religious, political, or racial slurs
- Any messages or content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Users are also not permitted to use the Internet in a way that could affect others' usage. This means not streaming or downloading media files and not using the Internet to play online games.

Other business use
Users are not permitted to use emails or the Internet to carry out their own business or the business of others. This includes, but is not limited to, work for political organisations, not-for-profit organisations, and private enterprises. The SIRO may lift this restriction on a case-by-case basis.

Security
Users will only use corporate accounts and systems in accordance with our Information Security Policy. In particular, users will not:

- Click on links from untrusted or unverified sources
- Use insecure email transmission methods when sending personal data
- Sign up for marketing material that could jeopardise our IT network
- Send excessively large email attachments without prior authorisation from the SIRO and/or our IT Provider
- Attempt to download any software onto corporate devices. This can present a virus risk and/or breach of software license requirements.

Group email accounts
Users may be permitted to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity, and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to the suspension of a user's email rights.

The SPOC will be responsible for allowing access to group email accounts. All email traffic to and from individual and group accounts may be monitored.

Social Media and Private Messaging Apps

We recognise and embrace the benefits and opportunities that social media can contribute to an organisation. However, we also recognise that social media poses a data protection risk due to its open nature and capacity to broadcast to many people quickly.

Corporate accounts
We may have social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about our business activities. Authorised users will be given the usernames and passwords to these accounts, which must not be disclosed to any other user within or external to the organisation. The SPOC will be responsible for allowing access to corporate social media accounts.

Corporate social media accounts must not be used to disseminate personal data in an open forum or by direct message. Doing so would be a contravention of our information governance policies and data protection legislation.

Corporate accounts must not be used in a way which could:

- Tarnish our reputation
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs
- Be construed as sexually explicit
- Be construed as political beliefs or commentary.

Personal accounts
We understand that many users will use or have access to personal social media accounts. Users must not use these accounts:

- During working hours
- Using corporate equipment
- To conduct corporate business
- To contact or approach our clients, customers, or partners
- Make posts that relate to us or refer to information gained through your role within the organisation
- Identify your role within our organisation.

Private messaging apps
Social messaging apps such as WhatsApp, Facebook Messenger, etc. must not be used for communicating any school or Trust business. Information held in non-corporate communication channels may be subject to FOIA if it relates to official business.

Telephone and Video Conferencing Use

We provide users access to telephone and video conferencing services to assist with communication and performing their duties.

Personal use
Whilst telephone and video conferencing services should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Usage must not tarnish our reputation or infringe on business functions
- We may monitor and access call history and recordings
- We reserve the right to suspend telephone and video conferencing usage at any time
- Telephone calls, video conference recordings, or transcripts may be disclosed under the Freedom of Information and/or Data Protection Legislation.

Inappropriate use
We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other business use
Users are not permitted to use these services to carry out their own business or the business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. The SIRO may lift this restriction on a case-by-case basis.

Appendix Three - Pupil Acceptable Use - Primary

Information for Parents and Guardians

Digital technologies have become integral to children's and young people's lives, both within and outside school. These technologies are powerful tools that open up new opportunities for everyone. They can stimulate discussion, promote creativity, and raise awareness, which promotes effective learning. Young people should always be entitled to safe digital and Internet access.

This Acceptable Use Agreement is intended to ensure that:

- pupils will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use
- our digital systems are protected from accidental or deliberate misuse that could put the security of our systems and users at risk
- parents and guardians are aware of the importance of e-safety and are involved in the education and guidance of young people regarding online behaviour.

Pupil Acceptable Use Agreement

I understand that I must use digital technology responsibly by doing the following:

- I will only use computers or tablets with permission from a teacher or a suitable adult.
- I will only use applications that a teacher or a suitable adult has allowed me to use.
- I will take care of the computer, tablet, and other equipment.
- I will ask for help from a teacher or a suitable adult if I am unsure what to do or think I have done something wrong.
- I will tell a teacher or a suitable adult if I see something that upsets me on the screen.

I have read and understand the above and agree to follow these rules when:

- I use the school systems and devices (both in and out of school).
- I use my own equipment outside of school in a way related to schoolwork, e.g. communicating with other pupils or teachers, accessing school email, website, etc.

If I break the rules, I might not be allowed to use a computer or tablet for schoolwork.

Pupil name:
Class:
Pupil signature:
Date:

Parent or Guardian Permission

As the parent or guardian of the named pupil, I give permission for my child to access the Internet and digital systems at school.

I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the Internet, both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that my child is safe when using the Internet and digital systems.

I understand that my child's activity on digital systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to use the Internet and digital technologies safely at home and will inform the school if I have concerns about my child's e-safety.

Parent or guardian name:
Parent or guardian signature:
Date: