MAYBURY PRIMARY SCHOOL

# Online Safety Policy

Updated:  Autumn 2025

Maybury Primary School

Believe. Achieve. Succeed.

engage enrich excel academies

# Key Details

**Designated Safeguarding Lead: Della Sullivan**
**Deputy Designated Safeguarding Lead(s) Amanda Merritt, Katie Gregory, Claire Melling**

**Safeguarding Governor: Mrs Judy Hall**

**Computing lead Governor: Mrs Judy Hall**

**Computing/Online Safety Leader: Rachel Frew**

**Date of next review: October 2026**

**This policy will be reviewed at least annually.**

**It will also be revised following any concerns and/or updates to national and local guidance or procedure**

# Maybury Primary School

| | |
|---|---|
| Produced: | Autumn 2014 |
| Reviewed: | October 2025 |
| To be reviewed: | October 2026 |

## Online Safety Policy

**Mission**

Our values-based school nurtures curiosity and creativity through an inspiring, broad and engaging curriculum, where learning is at the heart of all that we do. Our children learn to become resilient and self-assured in an environment where safety is outstanding. Everyone is challenged and encouraged to thrive and achieve as individuals, preparing them for their role as caring and active citizens in modern Britain.

**Vision statement**

Believe. Achieve. Succeed.

# 1. Aims and objectives

Maybury Primary School aims to:

- Safeguard and protect all members of Maybury Primary's community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

### 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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **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

# 2. 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

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so

The policy also takes into account the National Curriculum computing programmes of study

# 3. Roles and Responsibilities

### 3.1 The governing board

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

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

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

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

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

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

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### 3.2 The headteacher

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

### 3.3 The designated safeguarding lead

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

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Computing Lead, IT management company and other staff, as necessary, to address any online safety issues or incidents
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT management company to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT management company and other staff, as necessary, to address any online safety issues or incidents
- Conducting a security check and monitoring the school's ICT systems on a half termly basis
- 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 to the headteacher and/or governing board
- Dealing with any filtering incidents which are identified on Senso cloud
- The DSL's have conducted a Filtering and Monitoring review Checklist, with their IT Provider, to review ratings against the standards. This will be reviewed annually or where necessary.

This list is not intended to be exhaustive.

### 3.4 IT management company

The IT management company and Headteacher 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

### 3.5 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 (Appendix 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting on CPOMS.
- Following the correct procedures by seeking approval from headteacher- who will liaise with the IT Manager- in a situation where they may need to review the filtering and monitoring systems for educational purposes e.g. accessing blocked website. An effective filtering system needs to block internet access to harmful sites and inappropriate content but it should not unreasonably impact teaching and learning or school administration.
- Working with the 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'

This list is not intended to be exhaustive.

### 3.6 Parents/carers

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 from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre, https://www.internetmatters.org/
- Hot topics – Childnet International, https://www.internetmatters.org/
- Parent resource sheet – Childnet International, https://www.internetmatters.org/

## 4. Managing Internet Access

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Visitors are required to sign a visitor's agreement prior to use of school online technologies
- Staff must change passwords on a regular basis
- The school accesses support from Eduthing who provide advice on safer online practices and filtering.

## 5. Reducing Online Risks

Our school recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

## 6. E-mail

- Pupils and staff may only use approved e-mail accounts on the school system and must immediately tell a teacher or Online Safety co-ordinator if they receive offensive e-mail.
- Staff must not reveal personal details of themselves or others, or confidential information about school in e-mail communication, websites (including social networking sites) or in chat rooms.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. The forwarding of chain letters is not permitted.
- Communication between parents and staff will be via info@maybury.surrey.sch.uk, head@maybury.surrey.sch.uk or class e-mail address, or via Tucasi software system.
- The school has adopted 2FA for staff Office 365/email accounts. This means that should any staff fall victim to a phishing attack which compromises their work Office 365 account, the attacker will not be able to gain access to the account without physically being on the school site.
- It is important that staff continue to remain vigilant as 2FA will not protect other accounts that they may use for work purposes, such as 3rd party providers like CPOMS and Arbor

## 7. Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published.
The head teacher and Website Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

## 8. Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.

Pupils' full names will be avoided on the Web site,  including in blogs, and will not be used in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. Parents sign a consent form when their child starts school to give permission for photographs to be shared online or in the media.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

**Maybury Primary School recognises that Online Safety is an essential part safeguarding of our pupils both in school and at home.**

## 9. Vulnerable Pupils

Our school is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Our school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.

Maybury Primary School will seek input from specialist staff as appropriate, including the Inclusion leader, DSL and Designated Teacher.

## 10. Social networking

The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords

Pupils will be advised never to give out personal details of any kind which may identify them or their location

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils

Pupils will be advised to use nicknames and avatars when using social networking sites.

Pupils will be encouraged to report any problems they encounter if using any social networking site and these will be reported in the Online Safety log book.

## 11. Managing filtering

If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Lead.

The Online Safety Lead, in conjunction with Eduthing (the School’s ICT management and technical support provider) will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school uses software, (Senso) to monitor computer and tablet-based activities on pupil and staff logins. Alerts are sent to the headteacher if anything inappropriate is found.

## 12. Use of personal devices including Smart Phones:

Staff are required to lock personal phones in drawers or safes during teaching hours.

Staff should not contact parents directly using their personal phone (even on private number) but should instead go through the school office.
Children are not permitted to bring their personal mobile technology into school. However, this is at the discretion of the head teacher. Year 6 pupils who walk home alone may be permitted to bring a phone, however this must be labelled and kept in the school office or with class teacher during the day.

Personal Smart phones must never be used to take photographs of pupils.

Staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Any data, files or images that are believed to be illegal must be passed to the police as soon as practicable, including pornographic images of children, without deleting them.

Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy. The school follows the DFE guidance “Searching, screening and confiscation.”

## 13. Parents as employees

It is acknowledged that some staff also have children who attend the school. It is recognised that in these cases the staff fulfil a dual role of parent and employee.

Parents as employees should ensure that they uphold boundaries between the two roles and that their behaviour does not constitute a conflict of interest. For example, they must maintain the same level of confidentiality despite social expectations. Parent-staff should discuss any inter-role conflict with their line manager. At Maybury Primary School our policy is that staff who are also parents should make a clear distinction between their personal account and staff account and therefore preserve the privacy of other staff working at the school. They should adhere to the high expectations the school has for their personal conduct online.

## 14. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

**GDPR**

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the School Business Manager, then you can contact the DPO on the details below: -

Data Controller Name: Craig Stilwell
Data Controller Details: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Data Controller Email: dataservices@judicium.com

## 15. Authorising Internet access

All staff must read and sign the 'Staff Code of Conduct for ICT ' (Appendix 1) before using any school ICT resource

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems

Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Any person working on school premises using the school network will be asked to read and adhere to a '**Visitor Notice- ICT Acceptable Use / Code of Conduct '** form (Appendix 2) before being allowed access to the Internet. Visitors to the school will be provided with a guest username and password to log on to the school network, which will allow limited access to files and programs.

All persons accessing the school system will need to agree to Future Digital settings before being allowed access.

## 16. Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the Online safety policy is adequate and that the implementation of the Online safety policy is appropriate and effective. We complete annual Online safety /ICT usage questionnaires.

## 17. Handling Online safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff

Any complaint about staff misuse must be referred to the head teacher

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures

Pupils and parents will be informed of the complaints procedure.

Pupils and parents will be informed of consequences for pupils misusing the Internet.

## 18. Community use of the Internet

All use of the school Internet connection by community and other organisations shall be in accordance with the school Online safety policy.

# 19. Introducing the Online safety policy to pupils

- The children sign an Acceptable use policy annually which is displayed in their classrooms.
- Sanctions for inappropriate use of ICT by pupils will be dealt with using our school Online safety rules and sanctions
- Appropriate elements of the Online safety policy will be shared with pupils.
- Online safety rules will be posted in all rooms with computer access.
- Pupils will be informed that network and Internet use will be monitored.

# 20. Curriculum and Online Safety

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

Curriculum opportunities to gain awareness of Online safety issues and how best to deal with them will be provided for pupils.

Pupils will celebrate Safer Internet Week in February of each year with each class hosting a parent/ student joint workshop aimed at an age appropriate level in addition to Online safety lessons throughout the year.

Each half term, each year group uses ProjectEVOLVE’s Knowledge Maps as a fun way to create meaningful discussion and give valuable insight into the gaps in children’s understanding. Over the year the 8 strands are covered:

- Self-image and Identity: Understanding how identity is represented, changed, and managed online.
- Online Relationships: Navigating respectful, safe, and healthy relationships in digital spaces.
- Online Reputation: Managing how personal information is shared and perceived by others.
- Online Bullying: Recognising and responding to bullying behaviours.
- Managing Online Information: Critical evaluation and validation of online content.
- Health, Well-being and Lifestyle: Understanding the impact of technology on physical and mental health.
- Privacy and Security: Protecting personal data and securing online accounts.

- Copyright and Ownership: Understanding rules around using others' creative work.

The data collected from these Knowledge Map sessions are used to inform future planning and whole school assemblies ensuring a tailored curriculum for our children each year.

## 21. Staff and the Online safety policy

All staff have access to the School Online safety Policy via the S drive and school website and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user.  Discretion and professional conduct is essential.

Sanctions for inappropriate use of ICT by staff will be dealt with in line with the Disciplinary and Capability policy, with advice from the LADO where appropriate.

If staff have an online safety concern they should refer to Flow chart (Appendix 3)

## 22. Enlisting parents’ support

Parents’ and carers attention will be drawn to the School Online safety Policy in newsletters, the school brochure and on the school web site

Parents and carers will from time to time be provided with additional information on Online safety

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school

The Online Safety Lead will deliver annual parent workshops covering Online safety to ensure parents are kept up to date.

This policy will be approved by the Governing Body and reviewed at least annually.

## 23. Google Classroom

Google Classroom is a secure platform which only children belonging to the school, with current passwords, can access. This stops external threats from being presented to children.
Names of children making comments are displayed too, with no option to delete comments. This reduces the risk of cyber bullying as comments can be monitored by teachers and staff to know what is being said and by who.

In each classroom there is a stream that children can comment on. They can ask questions of their fellow pupils and teachers, but they unable to create new posts.

Teachers will post links to suitable websites to support research tasks to reduce the need to look elsewhere for information. Additionally, children can also comment individually on a piece of work as they submit it. Teachers can then feedback directly to students on that particular piece of work and list any areas they have excelled in or areas to look at again, providing instant feedback.

The purpose of our Google Classroom is to provide a safe and secure place to receive and share learning, and a place to connect with school staff and classmates. In Google Classroom, school staff can assign work to the students digitally, without paper. Google Classroom is accessible from any digital device with internet access and a web browser. Parents/carers can login and view the assignments that have been set, whether their child has completed and submitted them, and any feedback that they may have received.
Each year staff remind children of the rules for using Google Classroom ad follows:

- Do not share personal information such as e-mail, home address or phone number.
- Only login using your own username/login and password.
- During 'learning time', you will be expected to use Google Classroom to access, complete and submit learning. You should not use this time to access other content on the internet unless it is for the learning that is being done.
- Ask permission of a parent/carer when accessing content on different websites or apps.
- When submitting images, sound clips or video, make sure that these are appropriate for the learning task.

# 24. Cyber-bullying

### 24.1 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. (See also the school behaviour policy.)

### 24.2 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. This is though our online safety curriculum, Learning for Life curriculum, Online safety workshops and assemblies.

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.

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.

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.

# 25. Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (see 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/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

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher 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 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
- Our behaviour policy / touch and physical intervention 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.

# 26. The use of Artificial Intelligence (AI) systems in School

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR. We have DPIA's for all platforms.
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities. All teachers have completed Using AI in education settings DfE training.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- Children sign child friendly class AI agreement at school (Appendix 4).
- As set out in the Acceptable Use Statement – Staff Usage of AI and Artificial Intelligence Workforce Policy and Agreement staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school and with a DPIA in place may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, all systems have a DPIA in place which outlines tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school, for example parent workshops and newsletters.
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-

checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

## 27. Cybersecurity

“Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage”

The ‘Cyber-security in schools: questions for governing bodies and Trustees’ guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies’ and management committees’ understanding of their education settings’ cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (in partnership with Eduthing), has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school’s governance and IT policies reflect the importance of good cyber security
- staff and Governors receive regular training on the common cyber security threats and incidents that schools experience using BoxPhish and Eduthing.
- the school’s education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents.  All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.
- Half termly phishing simulations are deployed to provide training using BoxPhish.

# APPENDIX 1
# Staff and Governor

## ACCEPTABLE USE POLICY AND AGREEMENT

### Introduction

This policy is designed to enable acceptable use for staff and governors.
The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information. If you are in doubt and require clarification on any part of this document, please speak to the School Business Manager.

### Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.
The use of memory sticks and portable devices is strictly forbidden. Users must not install any software on the ICT systems- Software can only be installed by the schools IT provider, Eduthing. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The School Business Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.
Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

### Network access and security

All users of the ICT systems at the School must have a network user account, consisting of a username/e-mail address and a password. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the schools IT Provider, Eduthing, for the purposes of system support.

Two-factor authentication (2FA), is a security process in which users provide two different authentication factors to verify themselves. This is set up for all staff for when they try to access their Microsoft Account when not on the school network. 2FA is implemented to better protect both a user's credentials and the resources the user can access.

Users must report any security breach or suspected breach of their network, email or application account credentials to the School Business Manager or Headteacher as soon as possible. Users should only access areas of the school's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

**<u>School Email</u>**

Where email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during break times or after the working day, and must comply with this acceptable use policy. The School's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email. Work emails should be checked every working day. Where possible, emails should only be sent between the hours of 7:30am-6:30pm, it is not expected that you will respond to an email outside of these hours.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

## Internet Access

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Headteacher and /or School Business Manager.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral. Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.
If necessary such information may be handed to the police in connection with a criminal investigation.

## Digital photography and recording (including but not limited to images taken on Ipods, Ipads and cameras or equivalent devices)

The school encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

- Only children with the relevant consent should be photographed/ recorded. It is your responsible to check the consent for all children prior to capturing images/ footage.
- Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, smart watches iPads or similar.
- All photos should be downloaded to the school network as soon as possible.
- The use of personal mobile phones for taking photos of pupils is not permitted, only school devices may be used.

## File Storage

Staff members have their own personal area on the shared network, as well as access to shared network drives. Any school related work should be stored on one of these network drives and on desktops or home computers. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. No removable media, such as memory sticks, must be used. Home computers may be used but in accordance with the information access and security policy, summarised as follows:

- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be stored or transferred off site unless it is sent by secure email.

## Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The school provides equipment for this purpose.
- All phone contact with parents regarding school issues will be through the schools phones. If a staff member is working from home they should seek prior approval form the Headteacher to use a personal mobile to contact parents and their number must be with held at all times. Personal mobile numbers should not be given to parents at the school.

## Social networking

The School has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school’s reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Headteacher.
- Members of staff will notify the Headteacher or School Business Manager if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook). If, in exceptional circumstances, users wish to do so, please seek advice from the Headteacher or School Business Manager.

## Monitoring of the ICT Systems

The school uses Senso to monitor all usage across the school and exercises its right to monitor the use of its ICT systems. This monitoring software is installed to ensure that use of the network is regularly checked by the Headteacher and School Business Manager to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature. Monitoring also includes the ability to check websites accessed, the interception of e-mail and the viewing of data stored. Where it is believed that unauthorised use of the school's ICT system is, or may be taking place, or may be being used for criminal purposes relevant actions will be taken. Any inappropriate material found will be deleted unless pending a criminal investigation.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

## Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the school considers may amount to a criminal offence, or is unlawful, shall without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

# ACCEPTABLE USE AGREEMENT

To be completed by all staff,

As a school user of the network resources/ equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the school rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Headteacher or School Business Manager.

I agree to report any misuse of the network to the Headteacher or School Business Manager. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the Headteacher or School Business Manager. I agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Headteacher or School Business Manager.

Specifically when using school devices: -

- I must not use these devices for inappropriate purposes.
- I must only access those services I have been given permission to use.
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.
- I will support the schools Online Safety Policy and Child Protection and Safeguarding Policy and help pupils be safe and responsible when Online.
- I will ensure my actions are in line with the schools Safeguarding policies and procedures and will report any concerns to a DSL.
- I will ensure when I work from home it will be compliant with schools “Guidance note for staff working from home.”

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor activity in order to uphold this policy and to maintain the School’s network (as set out within this policy).

**Please review in conjunction with the Staff Behaviour (Code of Conduct) Policy**

Signed ………………………………………………. Date ………………..

Print name ……………………………………………………………………….

# **APPENDIX 2**
## **Visitor Notice- ICT Acceptable Use / Code of Conduct**

All visitors who are using school 'WiFi' or school ICT equipment ('The Service') are required to read the terms and conditions, as set out in this Acceptable Use/Code of Conduct. When you sign into school or start using 'The Service', you are deemed to have read, understood and agreed to the contents of this Acceptable Use/Code of Conduct. Any concerns or clarification should be discussed immediately with the school office, and before using 'The Service'.

I will only access the internet using the "MAY Guest" WiFi using the temporary password provided by the school office. I understand this temporary password will cease to work once I have left the premises.

I will only use the school's Internet and any related technologies for professional purposes.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

I will ensure that personal data is kept secure and is used appropriately on the school site and not taken off the school premises. The use of memory sticks or portable devices is strictly prohibited.

I will not install any hardware of software without permission.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

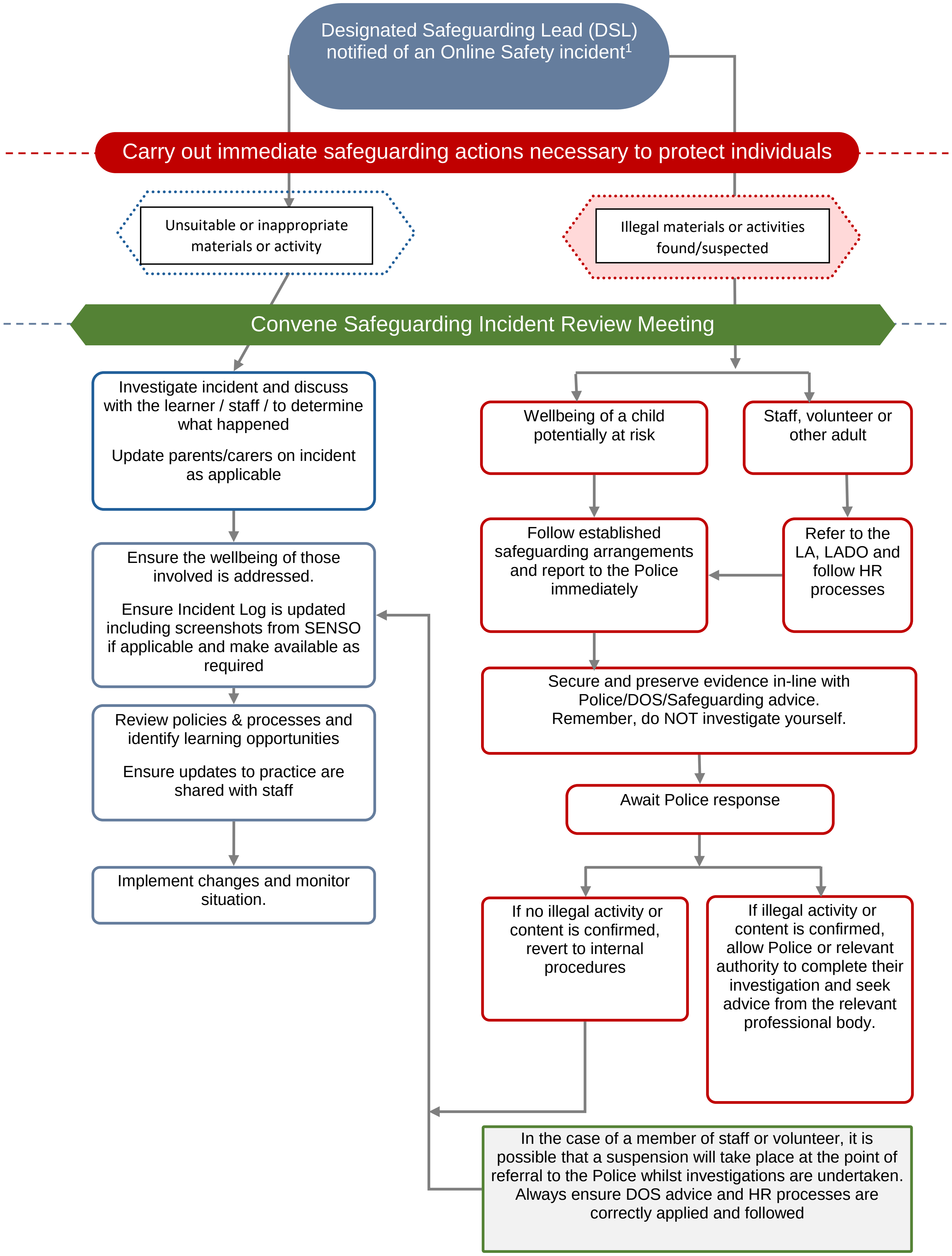
Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Head teacher.

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the Computing Lead, the Designated Safeguarding Leader or Head teacher.

# APPENDIX 3



Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]

Carry out immediate safeguarding actions necessary to protect individuals

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Investigate incident and discuss with the learner / staff / to determine what happened

Update parents/carers on incident as applicable

Ensure the wellbeing of those involved is addressed.

Ensure Incident Log is updated including screenshots from SENSO if applicable and make available as required

Review policies & processes and identify learning opportunities

Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Wellbeing of a child potentially at risk

Staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Refer to the LA, LADO and follow HR processes

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.

Await Police response

If no illegal activity or content is confirmed, revert to internal procedures

If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

## APPENDIX 4

# Maybury Primary School

*Believe. Achieve. Succeed.*

engage
enrich
excel
academies

## 🌞 Our AI Agreement 🌞

**(For Using AI Tools Safely and Kindly in School)**

This agreement helps us understand how to use AI tools safely, responsibly, and kindly in our classroom. AI tools can be fun and helpful, but we must use them the right way.

---

**👧🏾 👦🏼 I, ______________________________, agree to:**

1. ✅ **Use AI sensibly.**
   I know AI can help with learning, but I will always use it in a kind and sensible way.
2. ❌ **Remember that AI can get things wrong.**
   I understand that AI isn't always right – it can sometimes make mistakes!
3. 🔒 **Keep myself safe online.**
   I won't share my name, address, photos, or passwords with AI. I will also tell a trusted adult if something feels wrong.
4. 🔍 **Check facts.**
   I will check AI's answers using books, websites, or by asking my teacher – just to make sure they're correct.
5. 💙 **Take care of my feelings.**
   I know AI isn't a real person. I will talk to real friends and family if I feel upset or need help.
6. ⚖️ **Be fair and kind.**
   I know that sometimes AI might not be fair. I will always think about whether something is kind and respectful.
7. ✍️ **Do my own work.**
   I will use AI to help me learn, not to copy. I will always say when I've used AI in my work.
8. 🙋 **Ask for help.**
   If I'm not sure what to do, or something seems wrong, I will ask my teacher.
9. 🔴 **Tell someone if I see something wrong.**
   If someone is using AI in a mean or unsafe way, I will tell an adult I trust.
10. 🤔 **Stay curious and keep learning.**
    I will enjoy learning about AI, how it works, and how to use it in clever, careful ways!

---

### 🖊️ My Promise:

I promise to use AI safely, kindly, and responsibly.

**Signed:** ____________________________
**Date:** ______________________________