# HURST GREEN PRIMARY SCHOOL

# Online Safety Policy

**(previously known as E-Safety Policy)**

| Policy for the attention of | | | |
|---|---|---|---|
| Audience | Key Audience | Optional Audience | Additional/Notes |
| Senior Leadership Team | √ | | |
| Teachers | √ | | |
| Teaching Assistants | √ | | |
| Administrative Staff | √ | | |
| Lunchtime Supervisors | √ | | |
| Site Manager | | √ | |
| Cleaners | | √ | |
| Governors | √ | | |
| Parents | √ | | |
| Website | √ | | |
| Local Authority | | √ | |

| | |
|---|---|
| Responsibility of | School Improvement |
| Review frequency | Every two years from Autumn 2025 |
| Previous versions agreed | 1 February 2013; 3 February 2014; 21 March 2016; 6 February 2017; 5 February 2018; 4 February 2019; 3 February 2020; 22 February 2021; 7 February 2022; 6 February 2023; 19 February 2024 |
| This version agreed | 13 October 2025 |
| Next review date | Autumn 2027 |

## Contents

# Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Hurst Green Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

Our school's Online Safety Policy is designed to address current and emerging online safety issues within a whole-school context. It aligns closely with other key policies, including our Safeguarding Policy, Behaviour Policy, and Anti-Bullying Policy. Grounded in our core values of **respect, equity, aspiration, collaboration, responsibility,** and **compassion**, the policy aims to ensure a safe, inclusive, and supportive digital environment for all members of the school community.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Hurst Green Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

# Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff.

# Policy and leadership

## Responsibilities

To ensure the online safeguarding of members of our school community, it is important that everyone works together in a spirit of **collaboration** to develop safe and responsible online behaviours. By learning from each other and from good practice elsewhere, and by reporting inappropriate online behaviours, concerns, and misuse as soon as they arise, we promote a shared sense of **responsibility**.

While this is a team effort, the following sections outline the specific online safety roles and responsibilities of individuals and groups within the school.

## Headteacher and senior leaders

- 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 day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and Deputy head 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[1].
- 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 / Online Safety 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.

## Governors

The DfE guidance "Keeping Children Safe in Education" states:

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare- this includes online safety."

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 governors whose members 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 / Online Safety 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

## Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

> "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). This should be explicit in the role holder's job description."
>
> They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"
>
> They (the DSL) "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, but a Hurst Green we have an Online Safety Lead who works in support of the DSL in carrying out these responsibilities.

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

## Online Safety Lead

The Online Safety Lead will:

- Lead the Online Safety Group
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Have a leading role in establishing and reviewing the school online safety policies/documents
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- Liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

## Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

## Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding

- They have read, understood, and signed the staff acceptable use policy (AUP)
- They immediately report any suspected misuse or problem to the head teacher DSL for online safety for investigation/action, in line with the school safeguarding procedures
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. The guidance contained in the swgfl Safe Remote Learning Resource
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- They model safe, responsible, and professional online behaviours in their own use of technology, including outside of school and in their use of social media, demonstrating **respect** for themselves, others, and the wider school community.
- They are aware of both the benefits and risks associated with the use of Artificial Intelligence (AI) services in school, demonstrating **responsibility** and transparency in how these technologies are used. AI should support, not replace, human decision-making. Staff must ensure that all final judgments—particularly those affecting individuals—are made by humans, carefully fact-checked, and critically evaluated. The use of AI should reflect our **aspiration** to enhance learning and decision-making while maintaining ethical standards.

## IT Provider

The IT service provider should have technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- Procure systems
- Identify risk

- Carry out reviews
- Carry out checks

It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- The school technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE and guidance from local authority
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the head teacher for investigation and action
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- Monitoring systems are implemented and regularly updated as agreed in school policies

## Learners

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use policy (AUP) and Online Safety Policy
- 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 avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

## Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the learners' acceptable use agreement
- Publishing information about appropriate use of social media relating to posts concerning the school.
- A clear parental code of conduct, outlining parental responsibilities in regard to their own use of technology (particularly in relation to the school).
- Seeking their permissions concerning digital images
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to learners in school.
- Ensuring the safe and responsible use of their children's personal devices in the school (where this is allowed)

## Community users

Community users- or students- who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. (A community user's acceptable use agreement template can be found in the appendices).

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

## Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group has the following members (amend as appropriate):

- Designated Safeguarding Lead
- Online Safety Lead
- senior leaders
- online safety governor
- technical staff
- learners - digital leaders

Members of the Online Safety Group will assist the DSL/OSL with:

- The production/review/monitoring of the school Online Safety Policy/documents

- The production/review/monitoring of the school filtering policy and requests for filtering changes
- Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- Reviewing network/filtering/monitoring/incident logs, where possible
- Encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- Consulting stakeholders – including staff/parents/carers about the online safety provision
- Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

An Online Safety Group terms of reference template can be found in the appendices.

# Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- There is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence
- There is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial intelligence (ai) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- Policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.
- Where generative ai is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.
-

# Policy

## Online Safety Policy

**The DfE guidance "Keeping Children Safe in Education" states:**

**"Online safety and the school or college's approach to it should be reflected in the child protection policy"**

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- Describes how the school will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements
- Is published on the school website.

# Acceptable use

The school has defined what it regards as acceptable/unacceptable use, and this is shown in the tables below.

## Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be regularly promoted, understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices.

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- Staff induction and handbook
- Digital signage
- Posters/notices around where technology is used
- Communication with parents/carers
- Built into education sessions
- School website

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | **Any illegal activity for example:**<br>• Child sexual abuse imagery*<br>• Child sexual abuse/exploitation/grooming<br>• Terrorism<br>• Encouraging or assisting suicide<br>• Offences relating to sexual images i.e., revenge and extreme pornography<br>• Incitement to and threats of violence<br>• Hate crime<br>• Public order offences - harassment and stalking<br>• Drug-related offences<br>• Weapons / firearms offences<br>• Fraud and financial crime including money laundering | | | | | X |
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)<br>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices<br>• Using penetration testing equipment (without relevant permission)<br><br>N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here | | | | | X |

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs) | | | X | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | Using school systems to run a private business | | | | X | |
| | Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school | | | | X | |
| | Infringing copyright and intellectual property (including through the use of AI services) | | | | X | |
| | Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | X | X | |
| | Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |

| Consideration should be given for the following activities when undertaken for non-educational purposes:<br>Schools may wish to add further activities to this list. | **Staff and other adults** | | | | **Learners** | | | |
|---|---|---|---|---|---|---|---|---|
| | Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission/awar |
| Online gaming | | | | | | | | |
| Online shopping/commerce | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| File sharing | | | | | | | | |
| Social media | | | | | | | | |
| Messaging/chat | | | | | | | | |
| Entertainment streaming e.g. Netflix, Disney+ | | | | | | | | |
| Use of video broadcasting, e.g. YouTube, | | | | | | | | |
| Mobile phones may be brought to school | | | | | | | | |
| Use of mobile phones for learning at school | | | | | | | | |
| Use of mobile phones in social time at school | | | | | | | | |
| Taking photos on mobile phones/cameras | | | | | | | | |
| Use of other personal devices, e.g. tablets, gaming devices | | | | | | | | |
| Use of personal e-mail in school, or on school network/wi-fi | | | | | | | | |
| Use of school e-mail for personal e-mails | | | | | | | | |
| Use of AI services that have not been approved by the school | | | | | | | | |

When using communication technologies, the school considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.

- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) Must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

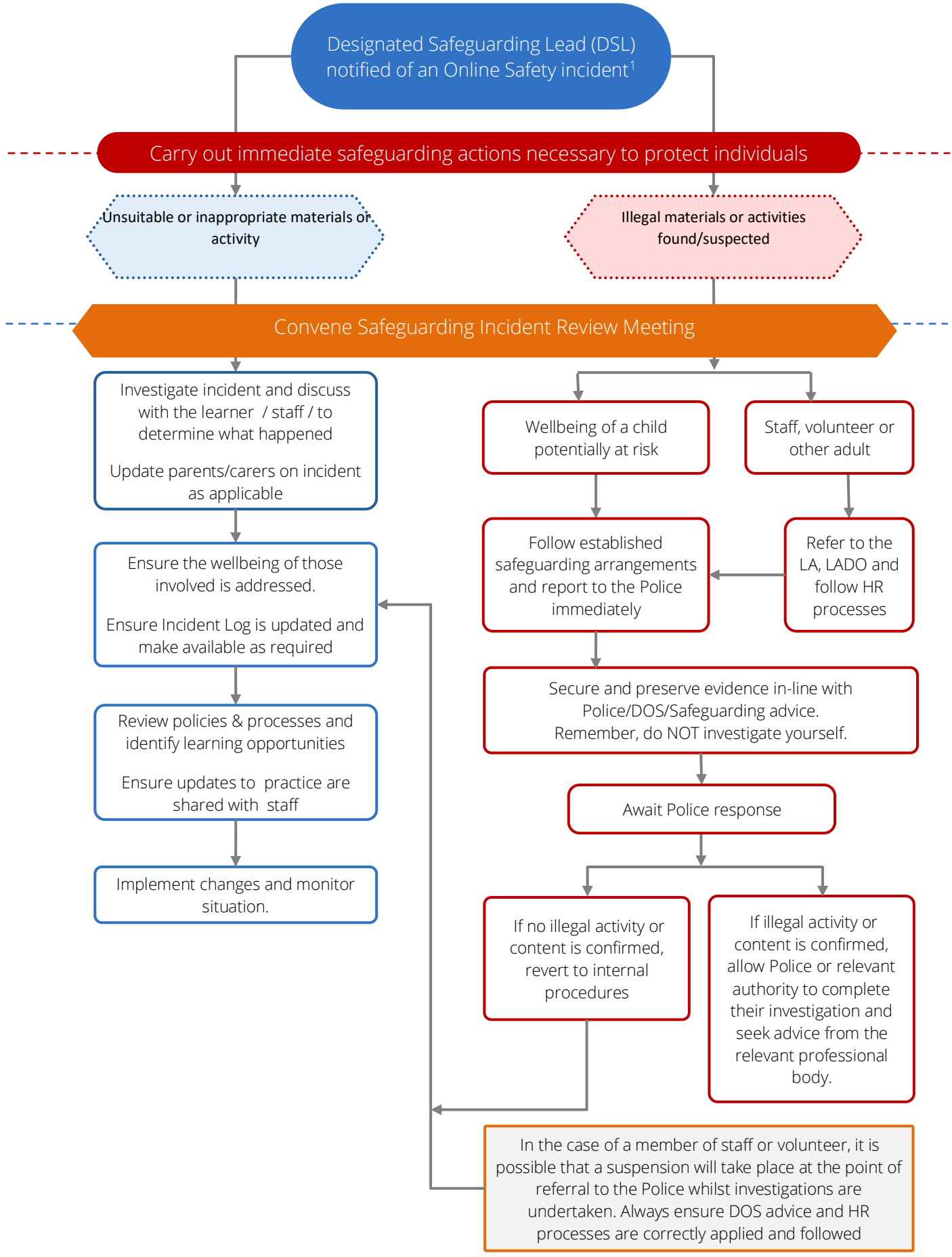
# Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents
- Reports will be dealt with as soon as is practically possible once they are received
- The designated safeguarding lead, online safety lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), 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
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority

- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - Internal response or discipline procedures
        - Involvement by local authority / MAT (as relevant)
        - Police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- Incidents should be logged
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. Local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- Learning from the incident (or pattern of incidents) will be provided to:
    - The Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - Staff, through regular briefings
    - Learners, through assemblies/lessons
    - Parents/carers, through newsletters, school social media, website
    - Governors, through regular safeguarding updates
    - Local authority/external agencies,

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


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 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

## School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

# The use of Artificial Intelligence (AI) Systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

## Policy Statements

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 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.

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.

As set out in the staff acceptable use 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.

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.

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.

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.

## Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is

therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the Cyber Choices site.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit
- It is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. Racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

## Contribution of Learners from Here

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- Mechanisms to canvass learner feedback and opinion
- Appointment of digital leaders
- Learners contribute to the online safety education programme e.g. Peer education, digital leaders leading lessons for younger learners, online safety campaigns
- Updating acceptable use agreements
- Contributing to online safety events with the wider school community e.g. Website information.

## Staff/Volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- The training will be an integral part of the school's annual safeguarding, data protection and cyber-security training for all staff
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- The online safety lead and designated safeguarding lead will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/inset days
- The designated safeguarding lead/online safety lead will provide advice/guidance/training to individuals as required.

## Governors

**Governors should take part in online safety training/awareness sessions**, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- Attendance at training provided by the local authority
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

**A higher level of training will be made available to (at least) the Online Safety Governor. This will include:**

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

## Families

Some parents and carers may have a limited knowledge of the risks and challenges associated with online safety. However, they play a vital role in educating their children and supporting the monitoring and regulation of their online behaviours. Parents can sometimes underestimate how frequently children and young people encounter potentially harmful or inappropriate material online, and they may feel unsure about how best to respond. By working in **collaboration** with the school, families can help create a safer and more informed online environment for all children.

The school will seek to provide information and awareness to parents and carers through:

- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- Regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- The learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons
- Letters, newsletters, website, learning platform,
- High profile events / campaigns e.g. Safer internet day
- Reference to the relevant web sites/publications, e.g. Swgfl; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers
- Sharing good practice with other schools in clusters and or the local authority

## Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- providing online safety information via their website and social media for the wider community

## Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is **responsible** for online safety and data protection.

## Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced.

## Filtering

A member of the SLT and a governor, are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.

The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering

standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the rm url filtering list and the police assessed list of unlawful terrorist content, produced on behalf of the home office. Content lists are regularly updated
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes
- Filtering logs are regularly reviewed and alert the designated safeguarding lead or online safety lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The dsl and governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- The school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- Access to content through non-browser services (e.g. Apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

## Monitoring

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the designated safeguarding lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours.

- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- Monitoring enables alerts to be matched to users and devices.

## Technical security

The school technical systems will be managed in ways that ensure that the school meets recommended standards:

- Responsibility for technical security resides with slt who may delegate activities to identified roles.
- A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually.
- all users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.
- Password policy and procedures are implemented and are consistent with guidance from the national cyber security centre
- All school networks, devices and system will be protected by secure passwords.
- The administrator passwords for school systems are kept in a secure place
- There is a risk-based approach to the allocation of learner usernames and passwords.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies in the cloud.
- The computing team is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on a school-owned devices without the consent of the slt/it service provider.
- Removable media is not permitted unless approved by the slt/it service provider.

- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- Guest users are provided with appropriate access to school systems based on an identified risk profile.
- Systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using artificial intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party ai systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- Dual-factor authentication is used for sensitive data or access outside of a trusted network using Microsoft authenticator

# Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- Security risks in allowing connections to your school network
- Filtering of personal devices
- Breakages and insurance
- Access to devices for all learners
- Avoiding potential classroom distraction
- Network connection speeds, types of devices
- Charging facilities

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

| | **School devices** | | | **Personal devices** | | |
|---|---|---|---|---|---|---|
| | School owned for individual use | School owned for multiple users | Authorised device[2] | Student owned | Staff owned | Visitor owned |
| Allowed in school | **Yes** | **Yes** | **Yes** | **Yes (certain groups)** | **Yes** | **Yes** |
| Full network access | **Yes** | **Yes** | **No** | **No** | **No** | **No** |
| Internet only | | | **Yes** | **No** | **Yes** | **Yes** |

## School owned/provided devices:

- All school devices are managed though the use of Mobile Device Management software
- There is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- Any designated mobile-free zone is clearly signposted
- Personal use (e.g. Online banking, shopping, images etc.) Is clearly defined and expectations are well-communicated.
- The use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- Liability for damage aligns with current school policy for the replacement of equipment.
- Education is in place to support responsible use.

[2] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

# Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- Ensuring that personal information is not published
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.
- Guidance for learners, parents/carers

**School staff should ensure that:**

- No reference should be made in social media to learners, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- They act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures.

## Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to personal social media sites during the day, but only when in areas away from pupils.

### Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies.

## Social networking by parents

Inappropriate use of social networking sites by parents Although social networking sites may appear to be the quickest and easiest way to express frustrations or concerns about the School (and those associated with it), it is rarely appropriate to do so. Other channels, such as a private and confidential discussion with the School, or using the School's formal complaints process are much better suited to this. The School considers the following examples to be inappropriate uses of social networking sites:

- Making allegations towards staff or children regardless of using names or not
- Making complaints about the school or staff
- Making defamatory statements about the school, staff or pupils
- Posting racist comments
- Posting photos of other children in school uniform without prior consent of all parties
- Posting comments that threaten violence

Parents should also ensure that their children are not using social networking/internet sites unless they are of the required age. It is expected that parents explain to their children what is acceptable to post online. Parents are also expected to monitor their children's online activity, including to their use of social media.

The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step, the school will usually discuss the matter with the parent to try and resolve the matter and to ask that the relevant information be removed from the

social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the school considers inappropriate, the school will consider taking further action.

## Unsuitable or inappropriate activities by pupils

Unsuitable or inappropriate activities If a child has been found to be using social media inappropriately, and it is reported to the school, the school has a right to take disciplinary action with reference to the school's behaviour policy. This can include a fixed term exclusion. This policy works in conjunction with other policies including the behaviour policy.

## Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those learners 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
- 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 learners in the digital/video images
- 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 learners are appropriately dressed
- Learners must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with online safety policy
- Written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- 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
- Images will be securely stored in line with the school retention policy
- Learners' work can only be published with the permission of the learner and parents/carers.

# Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by Juniper Websites. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

# Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- Has a Data Protection Policy.
- Implements the data protection principles and can demonstrate that it does so
- Has paid the appropriate fee to the Information Commissioner's Office (ICO)

- Has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- Has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- Information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- Provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- Has procedures in place to deal with the individual rights of the data subject,
- Carries out Data Protection Impact Assessments (DPIA) where necessary e.g. To ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests
- Provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- Data will be encrypted, and password protected.
- Device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- Data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- Only use encrypted data storage for personal data
- Will not transfer any school personal data to personal devices and staff will have to use 2f authenticators when offsite.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

# Cyber Security

"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 school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

- 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 their technology support partner), 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 training on the common cyber security threats and incidents that schools experience
- 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.

# Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- There is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- There are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and governors
- Parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- The evidence of impact is shared with other schools, agencies and las to help ensure the development of a consistent and effective local online safety strategy.

# School Online Safety Policy Appendices

## Appendix

## A1 Learner Acceptable Use Agreement Template – for KS2

I agree to use the school's digital systems safely and responsibly to protect me, other learners and the school.

**Keeping Safe Online**

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

**Using Computers and the Internet Sensibly**

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.

- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

**Being Respectful and Responsible**

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

**What Happens If I Break These Rules**

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.
-

Name of Learner:..... Group/Class:.....

Signed: ..... Date: .....

# A2 Learner Acceptable Use Agreement Template – for younger learners (Early Years/KS1)

**Our Technology Rules**

I will follow these rules to use computers, tablets and the internet safely at school.

**Staying Safe**

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

**Using Technology Kindly**

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

**Making Good Choices**

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

**What Happens If I Forget the Rules**

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

Signed (child): .....

# A3 Staff (and Volunteer) Acceptable Use Agreement Template

## School Policy

Digital technologies have become integral to the lives of everyone, including children and young people , both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

### For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies. .

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
  - will only use AI technologies approved by the school
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
  - will take care not to 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.
  - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
  - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing

    - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of the school.

- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

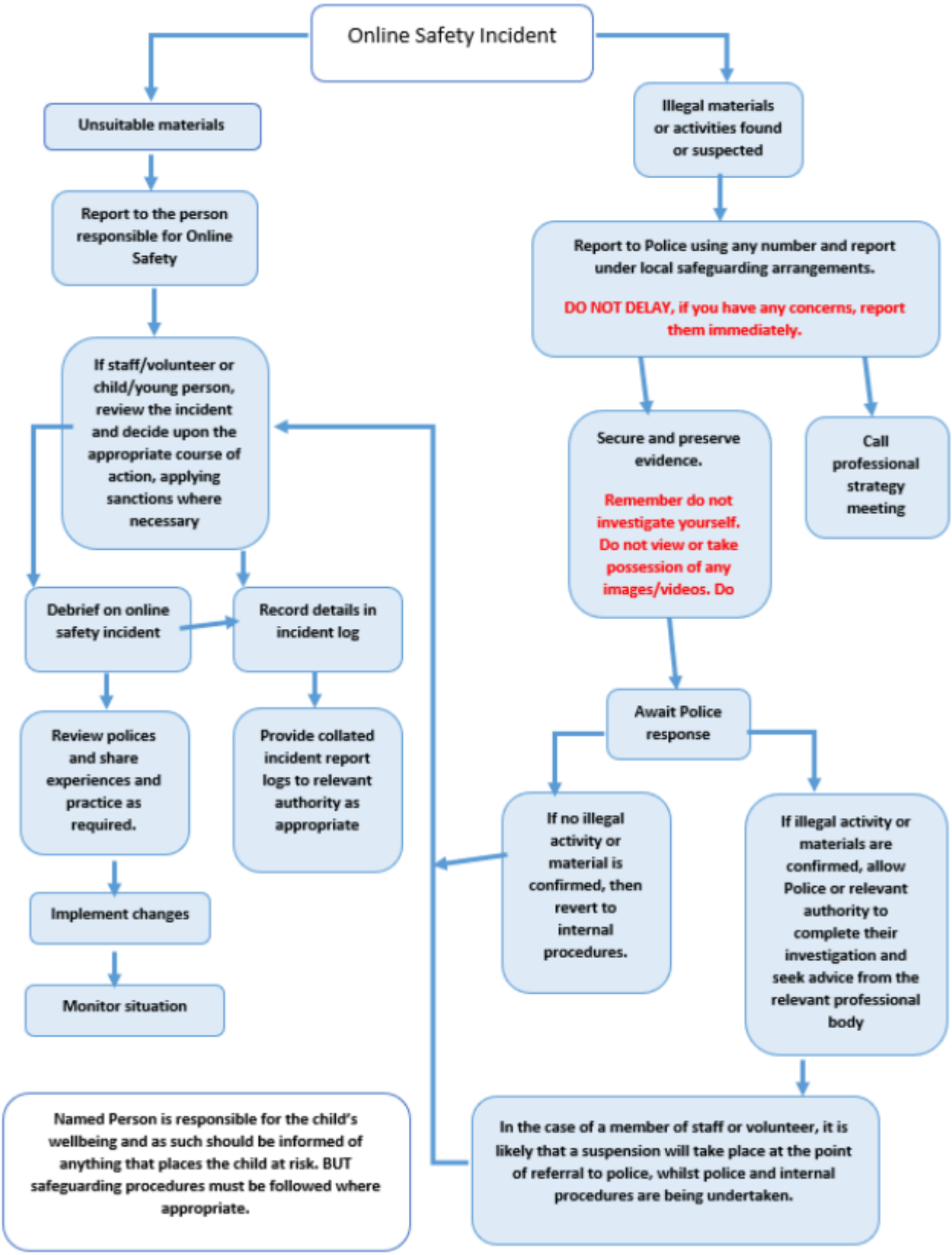
I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

# Appendix B1 Responding to incidents of misuse – flow chart



# Appendix C1 Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation. A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

**Computer Misuse Act 1990**

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

**Data Protection Act 1998**

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

**The Data Protection Act 2018:**

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.

- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

**All data subjects have the right to:**

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

**Freedom of Information Act 2000**

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

**Communications Act 2003**

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

**Regulation of Investigatory Powers Act 2000**

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
Establish the facts;
Ascertain compliance with regulatory or self-regulatory practices or procedures;
Demonstrate standards, which are or ought to be achieved by persons using the system;
Investigate or detect unauthorised use of the communications system;
Prevent or detect crime or in the interests of national security;
Ensure the effective operation of the system.
Monitoring but not recording is also permissible in order to:
Ascertain whether the communication is business or personal;
Protect or support help line staff.
The school reserves the right to monitor its systems and communications in line with its rights under this act.

**Trade Marks Act 1994**

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must

not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

**Copyright, Designs and Patents Act 1988**
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

**Telecommunications Act 1984**
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

**Criminal Justice & Public Order Act 1994**
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

**Racial and Religious Hatred Act 2006**
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

**Protection from Harassment Act 1997**
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

**Protection of Children Act 1978**
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

**Sexual Offences Act 2003**
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage

in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

**Public Order Act 1986**
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

**Obscene Publications Act 1959 and 1964**
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

**Human Rights Act 1998**
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:
The right to a fair trial
The right to respect for private and family life, home and correspondence
Freedom of thought, conscience and religion
Freedom of expression
Freedom of assembly
Prohibition of discrimination
The right to education
These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.
**The Education and Inspections Act 2006**
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

**The Education and Inspections Act 2011**
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

**The Protection of Freedoms Act 2012**
Requires schools to seek permission from a parent/carer to use Biometric systems

**The School Information Regulations 2012**
Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

**Serious Crime Act 2015**
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)
**Criminal Justice and Courts Act 2015**
Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners.

Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.
For further guidance or support please contact the Revenge Porn Helpline

## Appendix D1: Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations
Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign
Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media



Curriculum
SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools
Teach Today – www.teachtoday.eu/
Insafe - Education Resources
Data Protection
360data - free questionnaire and data protection self review tool
ICO Guides for Organisations
IRMS - Records Management Toolkit for Schools
ICO Guidance on taking photos in schools
Professional Standards/Staff Training
DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline
Infrastructure/Technical Support/Cyber-security
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.

NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes
Working with parents and carers
SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters
Prevent
Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me
Research
Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in schools and colleges
Further links can be found at the end of the UKCIS Education for a Connected World Framework