# AYSCOUGHFEE HALL SCHOOL

## ONLINE SAFETY POLICY

**Aims and Objectives**

It is the duty of Ayscoughfee Hall School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy applies to all members of the school community (including staff, pupils, parents/carers, visitors, volunteers and community users) is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Acceptable Use of AI
- Acceptable Use of IT
- Anti-bullying Policy
- Behaviour Policy
- Data Protection Policy and Privacy Notice/s
- Educational Visits Policy

DRAFT

- Mobile Phone Policy & Leaflet
- Prevent Risk Assessment/Action Plan
- PSHE / RSE Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct

At Ayscoughfee Hall School, we understand the responsibility to educate our pupils on online safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

**Scope**

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching staff, governors, and volunteers;
- "parents" includes pupils' carers and guardians; and
- "visitors" includes anyone else who comes to the school.

For the purpose of both this policy and the Acceptable Use policy, the term 'devices' refers to and covers any electronic, digital, wearable or internet-enabled device, either provided by the school or owned by staff, pupils or visitors and brought onto school premises, capable of one or more of the following functions:

- Making or receiving calls or messages;
- Accessing the internet or online services;
- Capturing, storing, transmitting or livestreaming images, video or audio;
- Recording conversations or other activities;
- Tracking location or personal data;
- Using artificial intelligence features to collect, process or transmit information;
- Connecting wirelessly to another device or network.

This includes but is not limited to, mobile phones, smartphones, tablets, smartwatches, smart glasses, wearable technology, earbuds with recording or communication functions, AI-enabled devices and any future technologies with similar capabilities.

In designing this policy, the school has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks outside of school. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's Behaviour Policy, Anti-bullying Policy, Mobile Phone Policy and / or Safeguarding and Child Protection Policy as is appropriate in the circumstances.

DRAFT

**Roles and responsibilities in relation to online safety**

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in in line with the Safeguarding and Child Protection Policy.

**The Governing Body**

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- All staff, in particular the Online safety Coordinator, DSL and Senior Leadership Team are adequately trained about online safety
- All staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified.
- Staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

The Safeguarding governor, Miss A Cole, works with the Online Safety Lead (Headteacher) to carry out regular monitoring in line with DfE Filtering and Monitoring Standards (March 2025), including the effectiveness of filtering and monitoring systems, and report to the Governors.

**Headteacher and the Senior Leadership Team**

The Headteacher is responsible for the safety of the members of the school community, and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for:

- Procuring appropriate filtering and monitoring systems.
- Documenting decisions on what is blocked or allowed and why.
- Reviewing the effectiveness of the filtering and monitoring provisions at least annually.
- Overseeing reports.
- Ensuring staff are appropriately trained.

**The Designated Safeguarding Lead (DSL)**

The DSL takes the lead responsibility for Safeguarding and Child protection at Ayscoughfee Hall School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL (or Deputy DSL in her absence) will ensure that this policy is upheld at all times, working with the Senior Leadership Team, Online Safety Co-ordinator and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

DRAFT

The DSL will work closely with the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that monthly checks are properly made of the system.

**Online Safety Lead**

The DSL (Headteacher) has responsibility for leading online safety across the school and as such will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The Online Safety Coordinator will monitor filtering and monitoring reports and will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the governing body. The Online Safety Lead meets regularly (usually half-termly) with the Governor responsible for online safety.

**Computing Subject Lead**

The school's computing subject lead, Mr R Hutton, has a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. He is responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. Alongside the Headteacher, he monitors the use of the internet and emails, maintains content filters, and will report inappropriate usage to the Headteacher (in role of Online Safety Lead/DSL).

**Teaching and support staff**

All staff are required to sign and return the IT Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL (Headteacher) and the Senior Leadership Team as appropriate.

All staff must participate in training as required/directed by the Online Safety Lead (Headteacher).

**Pupils**

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy.

**Parents and carers**

Ayscoughfee Hall School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

DRAFT

**Filtering and Monitoring**

**In general:**

Ayscoughfee Hall School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

The school subscribes to the Securly system for filtering and Senso system for monitoring, both of which are administered by our IT providers, ARK ICT. It is the decision of Ayscoughfee Hall School, taking into account the age of its pupils, to accept fully the filtering and monitoring settings recommend by Securly and Senso in terms of blocked content. The school believes this to be a measured and proportionate approach which is backed up by the evidence of our continued review of filtering and monitoring reports. This decision is reviewed annually and if a request for access is received. Access requests should be submitted to the Online Safety Lead/DSL (T Wright); decisions taken thereon are recorded and stored in the Safeguarding area of the school One Drive system.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The Online Safety Lead/Computing Subject Lead will check once per half term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. The log for checking the filtering and monitoring systems is stored in the Online Safety Folder on the Safeguarding Drive of the School's One Drive. The effectiveness and suitability of the filtering and monitoring systems is reviewed by the Safeguarding and/or Online Safety governor, the DSL and Online Safety Lead, looking at the records of the checks along with all other evidence, including online safety incident logs and Senso and Securly weekly report logs. Such a review will occur at least once each academic year and additionally in the following circumstances:

- There is a major safeguarding incident.
- There is a change in working practices; or
- If any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content as well as, but not limited to, the following:

- Drugs
- Gambling
- Social Media
- Social Networking
- Network Misuse
- Chat/Messaging
- Web Mail
- Intolerance

DRAFT

- Other search engines (no safe search)
- Streaming Media
- Games
- Health
- Uncategorized
- Malware
- E-commerce/Shopping
- Sexual Content
- Pornography
- Plagiarism
- Web ads

If there is a good educational reason why a particular website, application, or form of content should not be blocked teaching staff should contact the Online Safety Lead/DSL for their consideration.

The school will monitor the activity of all users across all the school's devices or any device connected to the school's internet server allowing individuals to be identified. In line with the school's Data Protection Policy and/or Privacy Notice/s, the Online Safety Lead / Computing Lead will monitor the logs daily (via email alerts) and weekly via reports. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the DSL/DDSL if they are teaching material which might generate unusual internet traffic activity.

**Staff:**

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the DSL/DDSL if they believe that appropriate teaching materials are being blocked.

**Pupils:**

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the Computing Lead/appropriate teacher or DSL. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should speak with their class teacher for assistance, who will then refer onto the Computing Lead and DSL.

DRAFT

## Education and training

### Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school.

All teaching staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff receive information about Online Safety as part of their safeguarding briefing on arrival at school.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

### Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE / RSE, by presentations in assemblies, visits such as Warning Zone for Year 6 pupils and regular workshops for the Lincolnshire Stay Safe Partnership for Years 2-6, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. From year 6 pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL and any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about

DRAFT

respecting other people's information and images etc. through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding, Anti Bullying and Behaviour Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying. Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

**Parents**

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school seeks to support parents in protecting their children when using electronic equipment at home by providing regular online safety updates and advice from online safety experts via ParentMail. This includes subscribing to the online safety expert Alan McKenzie who provides short videos for parents and half-termly online safety newsletters.

**Bring Your Own Devices (BYOD)**

**Staff**

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them

Staff are referred to the Staff Code of Conduct, Mobile Phone Policy and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Ayscoughfee Hall School are permitted to bring in mobile phones/personal devices for their own use. Staff are not allowed to have their personal devices switched on during the working day. They may use such devices in the main school staffroom only during break-times and lunchtimes.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct and Educational Visits policies.

Visitors may use personal devices on school premises only in accordance with the school's online safety and acceptable use policies. Personal devices must connect only to the school's guest Wi-Fi unless permission to access the main school network has been granted by the Headteacher. Devices must not be used to capture photographs, video or audio recordings on site unless expressly authorised for school purposes. No school data, personal data or

DRAFT

confidential information may be stored on personal devices. The school reserves the right to restrict or withdraw access where devices are used inappropriately or in breach of this policy.

**Pupils**

Pupils are not permitted to bring their own mobile devices to school; this includes mobile phones, tablets, laptops, smart watches or any other form of device that has internet access.

If pupils bring in mobile devices for use after school, parents must specifically inform the school office that this is happening. Devices must be kept switched off and must be handed in to the School Office at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

School mobile technologies made available for pupil use including laptops, tablets, cameras, etc. These are stored in classrooms (iPads) or the computer suite. Access is available only under direct supervision of a school adult (teachers/teaching assistants) and should be monitored at all times. Pupils are not permitted to use technology which has internet connectivity whilst unsupervised.

Pupils are responsible for their conduct when using school devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the Headteacher to agree how the school can appropriately support such use. The Headteacher will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

**Online Communications**

**Staff**

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer / recent alumni (i.e. pupils over the age of 18 who have left the school within the past 12 months) or parents of recent alumni using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, should not be shared with pupils or parents / carers and recent alumni. Under no circumstances may staff contact a pupil or recent alumni using a personal telephone number, email address, or other messaging system nor should pupils and recent alumni be added as social network 'friends' or similar.

The school recognises that within the school community, some members of staff are parents themselves or may be friends with parents outside school. In such circumstances, staff should follow the guidance set out in the school Mobile Phone policy and Staff Code of Conduct, ensuring that school business of any kind is never discussed on personal devices or social media or any other platforms.

DRAFT

Staff must immediately report to Headteacher (or Deputy Headteacher in her absence) 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. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Headteacher or Bursar.

**Pupils**

All pupils are issued with their own personal school email addresses for use on our network Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all schoolwork/homework assignments etc. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork/research purposes, pupils should contact the Online Safety Lead/Computing Lead for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the Headteacher/Deputy Headteacher.

**Use of social media**

**Staff**

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with schoolwork or business from school devices or whilst teaching or in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room or staff-only areas of school.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct and Staff Social Media Policy.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Ayscoughfee Hall School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

DRAFT

    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct, Staff Social Media or Child Protection and Safeguarding Policy.

**Pupils**

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils vary seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

**Data protection**

Please refer to the Data Protection policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and pupils are expected to save all data relating to their work to their school issued device or to the school's central server as per the Acceptable Use of IT policy.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the Bursar/Headteacher.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Coordinator/Headteacher.

**Password security**

Pupils and staff have individual school network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

DRAFT

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers),
- not write passwords down; and
- not share passwords with other pupils or staff.

**Safe use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the school's policy on official social media posting.

**Artificial Intelligence**

Ayscoughfee Hall School does not permit the use of generative AI tools such as ChatGPT on school devices / systems by pupils. The use of generative AI tools by staff is covered in the Use of AI Policy. In particular, personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.]

Ayscoughfee Hall School will evaluate the benefits and risks of any proposed use of generative AI by staff or pupils, with particular regard to risk associated with safeguarding, data protection and the possibility of bias and discrimination. Any approved use of AI will be kept under review and the school will remain alert to the possibility of unauthorised use.

**Misuse**

Ayscoughfee Hall School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour/Anti-bullying policies.

DRAFT

**Complaints**

As with all issues of safety at Ayscoughfee Hall School, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Headteacher in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to the school's DSL, Mrs T Wright or Deputy DSL Mrs J Jeffries, in accordance with the school's Safeguarding and Child Protection Policy.

DRAFT

**This policy has been updated and will be used in draft form pending formal ratification by the Board of Governors.**