Online-Safety Policy

Alwyn and Courthouse Federation

Approved by:	Executive Headteacher	**Date:**	October 2023
Last reviewed on:			
Next review due by:	Autumn 2024		

Introduction and Overview Rationale

Our school aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and governors
- Safeguard and protect the children and staff.
- Identify and support groups of children that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content

- being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Lifestyle websites promoting harmful behaviours
- Hate content

Contact

- being subjected to harmful online interaction with other users,
- peer-to-peer pressure
- commercial advertising
- grooming (adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes)
- Social or commercial identity theft, including passwords

Conduct

- personal online behaviour that increases the likelihood of, or causes, harm
- making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography)
- sharing other explicit images
- online bullying or aggressive behaviours
- copyright (little care or consideration for intellectual property and ownership)

Commerce

- risks such as online gambling
- inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

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

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

Roles and responsibilities

Role	Key Responsibilities
Governors/Safeguarding governor (including online safety)	To ensure that the school has in place policies and practices to keep the children and staff safe online. To approve the Online Safety Policy and review the effectiveness of the policy. To make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. To co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). To ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. To support the school in encouraging parents and the wider community to become engaged in online safety activities
The Executive Headteacher	The Executive Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Head of School / DSL / Business Manager	Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school Work with the Executive Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks (DSL) Work with the IT team to make sure the appropriate systems and processes are in place Work with the Executive Headteacher, ICT lead and other staff, as necessary, to address any online safety issues or incidents Manage all online safety issues and incidents in line with the schools' child protection policy Ensure that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy Ensure that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy Update and deliver staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs) Liaise with other agencies and/or external services if necessary Undertake annual risk assessments that consider and reflect the risks children face Provide regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
All staff	Maintain an understanding of this policy Implementing this policy consistently Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet, and ensure that children follow the school's terms on acceptable use (appendices 1 and 2) Know that the DSL is responsible for the filtering and monitoring systems and processes, and to report incidents of those systems or processes failing Work with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

IT Support (Report to Business Manager)	To report online safety related issues that come to their attention, to the DSL or business manager To manage the school's computer systems in line with policy -maintain passwords - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive
Parents/carers	Will be asked to provide consent for children to use the Internet, as well as other technologies Should know and understand the school's 'rules of appropriate use for the whole school community.' Notify a member of staff or the head of school of any concerns or queries regarding this policy Ensure their child has understood the acceptable use policy of the school's ICT systems and internet Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites: › What are the issues? – UK Safer Internet Centre › Hot topics – Childnet International › Parent resource sheet – Childnet International
Visitors	Ensure they are aware of the policy and supported to follow it If appropriate, they will be expected to agree to the terms on acceptable use.

Communication:

The policy will be communicated to staff/children/community in the following ways:

- Full policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and Courthouse children at the start of each year. Acceptable use agreements to be issued to the KS2 school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and children are given information about infringements in use and possible sanctions.
- DSL / Head of School acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to DSL or Head of School
- Any concern about staff misuse is always referred directly to the Head of School, unless the concern is about the Executive Headteacher or in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is a widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and children.

Education and Curriculum

Children will be taught about online safety as part of the curriculum:

All schools have to teach:

Relationships education and health education in primary schools

In **Key Stage (KS) 1**, children will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Children in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- By the **end of primary school**, children will know:
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet may also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety will be adapted for vulnerable children, victims of abuse and some children with SEND.

Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website.

Online safety will also be covered during parents' evenings and information events.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of school and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the head of school.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that our children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children know how they can report incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be during computing lessons, PSHE and assemblies.

All staff receive training on cyber-bullying, its impact and ways to support children, as part of safeguarding training.

The schools may send information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among children, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The senior leadership team can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or children,
- Is identified in the school rules as a banned item for which a search can be carried out,
- Is evidence in relation to an offence

Before a search, if the SLT member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other children and staff. If the search is not urgent, they will seek advice from executive headteacher or DSL.

- Explain to the child why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the child's co-operation

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

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

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

If inappropriate material is found on the device, it is up to the executive headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, the executive headteacher may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person,
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of children will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on children' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, children and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The Alwyn and Courthouse Federation recognises that AI has many uses to help children learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully children in line with our behaviour and safeguarding policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the schools.

Acceptable use of the internet in school

All staff are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by children, staff and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreement in appendices 1 and 2.

Children using mobile devices in school

Children in Courthouse may bring mobile devices into school, but must hand them into their class teacher at the start of the day. They are not to be used on the school premises.

Any use of mobile devices in school by children must be in line with the acceptable use agreement.

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

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring the school approved anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school business manager.

How the school will respond to issues of misuse

Where a child misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures or staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

Staff members will receive training (at least once a year) on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

Relevant refresher training as well as relevant updates will be shared as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure children can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the DSL and Executive Headteacher. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1

Acceptable use:

- All Staff, governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.

- All staff, governors and visitors understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner.

- No staff, governors or visitors will disclose any passwords provided to them by the school.

- All staff, governors and visitors understand that they are responsible for all activity carried out under their username.

- Staff, governors and visitors will not install any hardware or software on any school owned device without the Executive Headteacher's permission.

- All staff, governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it to the Designated Safeguarding Lead as soon as possible.

- All staff, governors and visitors will only use the school's email / internet / school server etc and any related technologies for uses permitted by the Executive Headteacher or Governing Body. If anyone is unsure about an intended use, they should speak to the Executive Headteacher beforehand.

- All staff, governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Executive Headteacher or Governing Body.

- Personal devices must only be used in the context of school business with the explicit permission of the Executive Headteacher. Personal mobile phones or digital cameras must NEVER be used for taking any photographs related to school business.

- All staff, governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All staff, governors and visitors will only use the approved email system for school business.

- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use.

- Memory sticks should be password protected or encrypted.

- All staff, governors and visitors will make every effort to comply with copyright and intellectual property rights.

- All staff, governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Designated Safeguarding Lead in line with our school's Safeguarding and Child Protection Policy.

Unacceptable use

- Allow anyone else to use their allocated personal user ID and password on any school IT system.

- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected.
- Perform any unauthorised changes to IT systems or information.
- Attempt to access data that you are not authorised to use or access.
- Connect any non-authorised device to the network or IT systems.
- Store data on any non-authorised equipment.
- Give or transfer data or software to any external person or organisation without the authority of the school.
- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which is considered offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Place any information on the Internet that relates to the school, alter any information about it, or express any opinion about unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally
- Remove or disable anti-virus software.

This policy is linked to our Data Protection policy.

I acknowledge I have received a copy of the Acceptable Use of Technology Code of Conduct.

Full Name _____

Signature _____

Date _____

Appendix 2

The aims of this Acceptable Use of IT Policy are to:

- ensure that children benefit from all learning opportunities offered by the computing and internet resources provided by the school in a safe and controlled manner,
- give children clear guidance on safe and acceptable use of these resources
- make children aware that Internet use in school is a resource -if the resource is abused, then access will be denied.

General

- Virus protection software is used and updated on a regular basis.
- The DSL is the appointed member of staff responsible for e-safety.

Children' Access to the Internet:

- We use a "filtered and protected" Internet Service, which will minimise the chances of children encountering undesirable material.
- We will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen.
- Members of staff will be aware of the potential for misuse and will be responsible for explaining to children, the expectation we have of children.
- Teachers will have access to children' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.

Expectations of Children using the Internet:

- With age related support, we expect all children to take increasing responsibility for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Children using the Internet are expected not to deliberately seek out offensive materials. Should any children encounter any such material accidentally, they are expected to report it immediately to a teacher.

- Children are expected not to use any rude language in their communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.

- Children must ask permission before accessing the Internet or use a device.

- Children will not access social networking sites unless expressly permitted by the school or as part of a specific learning activity.

- Children should not access other people's files or programmes unless permission has been given.

- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

- No applications may be downloaded to the school's computers from the Internet or brought in on portable media from home for use in school.

- School work completed at home may be brought in on portable media or emailed, but this must be virus scanned by the class teacher before use.

- Personal printing is not allowed on the school network.

- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

- The school encourages the use of anti-virus software on machines used at home.

- Children consistently choosing not to comply with these expectations will be warned and subsequently, may be denied access to Internet resources.

School Website

The website will be regularly checked to ensure that there is no content that compromises the safety of children or staff.

The publications of children's work will be decided by a teacher.

The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website or social media without parental permission.

The school website will avoid publishing the full names of individuals in a photograph.

The school will ensure that the image files are appropriately named and will not use children' names in image file names if published on the web.

Personal Devices

Children may only use their own technology in school as part of a pre-arranged educational activity, with permission from a member of staff and authorised by the ICT Leader.

Inappropriate use is in direct breach of the school's acceptable use policy.

Acceptable Use Policy - All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.

Appendix 3

Online safety training needs audit	
Name of staff member:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	