Online Safety Policy

Date: **January** 2021

Review date: **January** 2022

Aims

This policy applies to all members of our school community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors, and community users) who have access to our digital technology, networks, and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

This policy is based on the Department of Education's (DfE) 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
- Searching, screening and confiscation
- Protecting children from radicalisation

The policy reflects the Equality Act 2010 and Education Act 2011, the latter of which has given education professionals stronger powers to tackle cyberbullying by not permitting the use of personal devices in school.

Our school aims to:

- Have robust processes in place to ensure the online safety of our pupils, staff, volunteers, and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community and its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Continually update and tighten the filtering system in place on all school electronic devices

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The school Designated Safeguarding Lead (DSL) will handle referrals to local authority multi-agency safeguarding hubs (MASH) and the Headteacher will normally handle referrals to the Local Authority Designated Officer (LADO). The LA, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this policy, there are links on our website for external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud, which might be useful to share with parents, and anonymous support for children and young people.

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline; to use technology for teaching and learning, and to prepare for life after school; and to immediately report any concerns or inappropriate behaviour, to protect pupils, their families, our staff and the reputation of the school and our Trust.

Academy Council

Key responsibilities:

- Formally receive this policy and review its effectiveness by following the proforma as outlined by the UK Council for Child Internet Safety (UKCIS): *Online safety in schools and colleges in the questions from the Governing Board*
- Ensure an appropriate senior member of staff, from the School Leadership Team (SLT), is appointed to the role of DSL, with lead responsibility for safeguarding and child protection (including online safety)
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Monitor that regular strategic reviews between DSL and SLT are taking place

- Incorporate online safety into Academy Council safeguarding discussions as appropriate
- Ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Ensure that policies and procedures are consistently followed by all staff and ensure that staff are aware of reporting procedures in an event of an online safeguarding incident
- Liaise with the DSL on all online-safety issues which might arise and to receive regular updates on school issues and broader policy and practice information
- Ensure the school implements and makes effective use of appropriate ICT systems and services, including school-safe filtering and monitoring, protected email systems and that all technology, including cloud systems, are implemented according to child-safety first principles
- Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead (DSL)

Key responsibilities:

- The DSL should take lead responsibility for safeguarding and child protection (including online safety)
- Ensure that all school staff understand this policy and that it is implemented consistently throughout the school
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Work with the Trust Head of Business Support, IT Technician, and other staff, as necessary, to address any online safety issues or incidents
- Stay up to date with the latest trends in online safety, including 'self-harm bullying' and getting undressed on camera
- Ensuring that any online safety incidents (including cyber-bullying) are logged and labelled as such in MyConcern/CPOMS as appropriate and dealt with appropriately in line with this policy
- Communicate regularly with SLT and the designated Safeguarding (and online safety) Governor to discuss current issues (anonymised), review incident logs and filtering/change control logs

IT Technician

Key responsibilities:

- Implementing appropriate content filtering and monitoring systems, which are updated on a regular basis to keep pupils safe from harmful, inappropriate content, including terrorist and extremist behaviour
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents (including cyber-bullying) are logged and labelled as such in MyConcern/CPOMS as appropriate, and dealt with appropriately in line with this policy

All staff

Key responsibilities:

- Ensure that all school users understand this policy and ensure that it is implemented consistently throughout the school

- Agree and adhere to the terms of acceptable use of the school's IT systems and internet, ensuring that pupils follow them
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, making the most of unexpected learning opportunities as they arise
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues, such as copyright and data law
- Prepare and check all online sources and resources before using them within the classroom
- Encourage pupils to follow the Acceptable Use Policy (AUP), remind them about it and enforcing school sanctions for breaches of the policy
- Notifying the DSL of new trends and issues before they become a problem
- Ensuring that any online safety incidents (including cyber-bullying) are logged and labelled as such in MyConcern/CPOMS as appropriate, and dealt with appropriately in line with this policy

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil AUP annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they, or someone they know, feel worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practices when using digital technologies outside of school and realise that the school's AUP covers actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental AUP and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting negative, threatening, or violent comments about others, including the school staff, volunteers, governors, contractors, pupils, or other parents/carers

Volunteers and contractors

Key responsibilities:

- Read, understand, sign, and adhere to the AUP (where appropriate)
- Report any concerns, no matter how small, to the DSL
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible, and professional behaviours in their own use of technology

Handling online safety concerns and incidents

Online safety concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should talk to the DSL if they are concerned about a pupil, to contribute to the overall picture or highlight what might not yet appear to be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside the classroom

(particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Peer on Peer Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policy (AUP)
- Data Protection Policy, agreements, and other documentation (e.g., privacy statement and consent forms for data sharing, image use, etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL on the same day – where clearly urgent, it will be reported by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the complaint is referred to the Chair of the Academy Council and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline: 0800 0280285

The school will actively seek support from other agencies as needed e.g. the UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, the Prevent Officer, the police, the Internet Watch Foundation (IWF).

We will inform parents/carers of online-safety incidents involving their children, and the police where staff or pupils engage in, or are subject to, behaviour which we consider is particularly disturbing or breaks the law

Educating and the curriculum

Pupils will be taught about online safety as part of the curriculum in line with the computing programmes of study as outlined in the national curriculum standards.

From September 2020, all primary schools will have to teach relationships and health education.

Pupils in Key Stage 2 will be taught:

- How to use technology safety, responsibly and respectfully
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships, as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter in all contexts, including online, whom they do not know

Online safety is also embedded into our special school curriculum. Where appropriate, the pupils follow the national curriculum programmes of study. For those pupils where this is not appropriate, online safety is delivered in a context which is in line with the age, stage, ability and need of the pupils.

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

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications and in information via the school website. This policy will also be shared with parents via the website.

Online safety will also be covered in sessions/workshops set up to inform parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

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

Any concerns about a child will be logged in the online portal MyConcern/CPOMS as appropriate, in line with the school's Safeguarding policy.

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 one 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 pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Classroom staff will discuss cyber-bullying with their tutor groups.

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

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads, and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the SLT to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

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

Social media incidents

Rules and expectations of behaviour for children and adults in our school community are governed by the school's AUP and Social Media Policy.

Breaches will be dealt with in line with the school Behaviour Policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Acceptable use of the school network and internet

All pupils, parents, staff, volunteers, and academy council members are expected to sign the relevant AUP for them before accessing the school's ICT systems and internet.

The use of the school's internet must be for educational purposes only, or for the purposes of fulfilling the duties associated with an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Pupils may bring mobile devices to school, but, in our primary schools, pupils are required to hand them in at reception on arrival and collect them at the end of the school day. A book is signed by the pupil to confirm that a mobile has been left at reception and is crossed off when collected.

In our special schools, pupils can bring mobile phones into school, but they are not permitted to use them during lessons, or any other activities organised by the school. Any use of mobile devices by pupils must be in line with the AUP.

Any breach of the AUP by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

In line with the DfE guidance *'Searching, screening and confiscation: advice for schools'*, the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the contents of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Staff using work devices outside of school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. This also applies to school email accounts linked to other mobile devices such as phones which must be password protected.

If staff have any concerns over the security of their device, they must seek advice from the IT Technician.

Work devices must be used solely for work activities.

Misuse of school technology

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both in and outside of school). These are defined in the relevant AUP, as well as well as the Personal Device Policy.

Where pupils contravene these rules, the school Behaviour Policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

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

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

The DSL 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 about 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. They will log concerning behaviours in line with our Safeguarding Policy using the online portal My Concern/CPOMS as appropriate.

This policy will be reviewed annually by the Headteacher. At every review, the policy will be shared with the Academy Council.

Links to other polices

This policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Policy and Procedures
- Data Protection Policy and Privacy Notices
- Complaints Policy

- Acceptable Use of Technology Policy (AUP)

Appendices

Appendix 1a – Pupil and Parent/Carer Acceptable Use Agreement Template for EYFS/KS1

Name of pupil:	
This is how we stay safe when we use computers: • I will ask a teacher or suitable adult if I want to use the computers/tablets • I will only use activities that a teacher or suitable adult has told or allowed me to use • I will take care of computers/tablets and other equipment • I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong • I will tell a teacher or suitable adult if I see something that upsets me on the screen • I know that if I break the rules, I might not be allowed to use a computer/tablet **I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 1b - Pupil and Parent/Carer Acceptable Use Agreement Template for KS2, KS3 and KS4

Name of pupil:

I will read and follow the rules in the Acceptable Use Agreement Policy

When I use the school's ICT systems (e.g. computers) and get onto the internet in school, I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address, or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I am finished working on it

I will not:

- Access any inappropriate websites, including social networking sites, chat rooms and gaming sites, unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log into the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement Template for Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, share, link to, or send such material) • Use them in any way which could harm the school's and Trust's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I am not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's Data Protection Policy. I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a pupil informs me that they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**