Last Updated | 14/09/23

September 2023 – September 2024

E-Safety Policy

WATERTON
ACADEMY TRUST®

Contents

1. Our School

1.1 Our Vision

Grow. Achieve. Shine - These are much more than words or a motto. At Churchfield Primary School we enable all children to **grow** as independent learners, **achieve** more than they ever believe they could and **shine** as unique individuals. Our school is a very special place, having been the beating heart of our community for over 120 years, we respect the lessons of the past whilst looking to the difference we can make in the future. Preparing our pupils for life in an ever-changing world, developing curious, well-rounded individuals who are determined to succeed.

1.2 Our Values

We are proud, and work hard to be the best that we can be

We are determined and resilient, embracing all challenges

We collaborate well, treating everyone as equals

We are honest, kind and show integrity

We respect all people, property and the environment

We believe in ourselves and strive for our goals

1.3 Our Golden Rule

1.4 Our School Aims

Our school aims are underpinned by our values. Through our school values, we aim to:

1. Promote high standards of academic and vocational achievement for every child, every time, through a highly-inclusive approach.
2. Promote a holistic view of the whole child, supporting them to become well-rounded individuals and members of society.
3. Encourage all children to develop positive relationships with, and respect for, themselves, each other, our local community and the wider world.
4. Provide a safe, welcoming and positive environment for our children and families; acting as a hub at the heart of our community.

1.5 Our Community

Bricks and mortar do not make a school, people do. We can achieve great things when we work together, and our community is at the heart of what we do. We are a hub of support for our families, and provide a safe and loving environment for our children to shine.

1.6 Our Academy Trust

Since December 2019 we have been a proud member of Waterton Academy Trust, providing even more opportunities for our pupils to shine. As part of the Waterton family, we ensure that success for all is not a goal, but an expectation.

2. Policy Summary

2.1 Policy Introduction & Rationale

At Churchfield Primary School, the safety of our pupils is paramount. In today's society, online safety is absolutely pivotal . We believe that it is important that children are educated on how to be safe online, whilst also being taught how to use the internet for good. We aim to provide a safe place in which our pupils learn to take a full part in society and learn to handle the risks and responsibilities inherent in adult life. As part of this and to achieve these aims teachers need to create the right balance between protecting pupils, securing ICT systems and improving access to systems and the internet.

2.2 Policy Aims

This policy is underpinned by the central aims of Churchfield Primary School and the values held by the school community. This policy aims to:

- Provide information for all stakeholders on how school delivers 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')
- Provide information for all stakeholders on the robust processes in place to ensure the online safety of all pupils
- Provide information for all stakeholders on the mechanisms to identify, intervene and escalate an incident, where appropriate

2.3 Inclusivity Statement

At Churchfield Primary School we use an inclusive approach to all aspects of education. Our aim is to always involve all children and stakeholders in all areas of the curriculum and school life. In accordance with the SEND Code of Practice, we recognise that this may mean making special adaptations or arrangements from time to time for children with specific disabilities. We welcome the involvement of disabled adults in all areas of school life.

3. Legalities & Linked Documents

3.1 Linked School & Trust Policies

This policy should be read in conjunction with the following policies and other linked policies:

- Safeguarding Policy
- Health & Safety Policy
- Anti-Bullying Policy
- Social Media Policy

3.2 Linked National & Local Documents

The policy has been developed in accordance with the following legislation and guidance:

- Working together to Safeguard Children
- Keeping Children Safe in Education
- DFE Teaching online safety in schools
- DFE Preventing and Tackling Bullying
- DFE Cyber-Bullying: Advice for Headteachers and School staff
- DFE Relationships and Sex Education
- DFE Searching, Screening and Confiscation
- DFE Prevent Duty
- Education Act

4. Key Responsibilities

4.1 Headteacher Responsibilities

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

4.2 Designated Safeguarding Leader Responsibilities

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Safeguarding & Child Protection policy. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

4.3 Waterton Academy Trust IT Services Manager Responsibilities

The WAT IT Services manager is Ian Burns, who may also disseminate responsibilities to Mint IT Support and technicians. The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

4.4 The Academy Standards Committee Responsibilities

The ASC has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The ASC will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). All governors will:

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

appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

4.5 All Staff Responsibilities

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

4.6 Parent Responsibilities

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Further support and information for parents is available in this policy.

4.7 Visitors

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. The 4 Key Categories of Risk

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

5.1 Content

Being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremis.

5.2 Contact

Being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

5.3 Conduct

Personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.

5.4 Commerce

Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

6. Resources for Parents & Staff

6.1 National Online Safety

School has a subscription to the National Online Safety platform (also known as the National College). All parents have access to both the national online safety mobile app, parent guides for different games and platforms, as well as a wealth of webinars and short CPD to further support parents and staff.

6.2 Useful Links

The following links may also be useful for parents:

- ChildNet
- Help & Advice for Parents
- UK Safer Internet Centre
- NSPCC E-Safety
- Think U Know
- National Online Safety Guides

7. Online Safety Education

7.1 Educating Pupils About Online Safety

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

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

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

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- 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 will 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 pupils with SEND.

7.2 Educating Parents About Online Safety

School will raise parents' awareness of internet safety in letters, other communications home, a weekly e-safety update and through themed information sessions. We will also give all parents access to information and CPD via our website and National Online Safety application. This policy will also be shared with parents. School will let parents 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 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.

8. Cyber Bullying

8.1 Definition

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

8.2 Preventing & 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. School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, we will follow the processes set out in the WAT Anti-Bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

8.3 Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL / appropriate staff member
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

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

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

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

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

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

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

9. Acceptable Use of School Networks

All pupils, parents, staff, volunteers and governors are expected to adhere to the acceptable use of the school's ICT systems and the internet. Visitors will be expected to adhere 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

10. Staff Using Work Devices Off-Premises

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 with a strong password

- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing any relevant security updates

Staff members must not use the device in any way which 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 IT Manager or Mint IT Support.

11. 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 (for example through emails, e-bulletins 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 pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils 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.

12. Filtering & Monitoring

School uses a robust filtering and monitoring system, provided through our ISP 'School's Broadband'. School's Broadband is a specially designed and dedicated connection, built for schools. The School's Broadband web filtering solution subscribes to the Internet Watch Foundation URL and Home Office Terrorism Block List. We operate a safety-first approach in school, with many sites blocked as standard. We have robust systems for both filtering and monitoring online activity using our academy devices, which is aligned with the DfE's filtering and monitoring standards (March 2023). Staff are alert to the risks posed to pupils via their use of technology, typically referred to as 'the four Cs' (content: harmful or illegal content; contact: harmful online interaction with other users; conduct: personal online behaviour that causes harm or increases the risk of harm; commerce: risks such as online gambling or phishing). Staff receive appropriate training, including related to the academy's filtering and monitoring systems, to support them in ensuring that any online risks are swiftly identified and reported. The Designated Safeguarding Lead takes lead responsibility for coordinating our response to any risks linked to online safety, and has a full awareness and oversight of reporting of concerns from our filtering and monitoring systems. Any risks identified for our pupils

arising from reports from either system will be responded to in line with this policy, and, additionally, our behaviour policy, as required, and, where needed, escalated to local agencies for additional support in line with local thresholds.

School receives daily filtering and monitoring reports with blocked sites, as well as using machine-learning to detect potential threats as soon as they emerge.

A1. Appendix 1 – Pupil & Parent Acceptable Use Policy

Parent/Carers - By proxy of accepting a place at Churchfield Primary School 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 below for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Pupils - When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it
- Not open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Not use any inappropriate language when communicating online, including in emails
- 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
- No arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

A2. Appendix 2– Staff, Visitors & Volunteers Acceptable Use Policy

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 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'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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.
- Agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- 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.
- Let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me 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.
- Always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

This form requires no signature and is agreed by proxy of accepting employment, voluntary work or visiting Churchfield Primary School.