Unique Policy Number: 50

Online Safety Policy

The Children's Endeavour Trust comprises:
Abbot's Hall Community Primary School
Bosmere Community Primary School
Broke Hall Community Primary School
Chilton Community Primary School
Combs Ford Primary School
Freeman Community Primary School
Springfield Junior School
Whitehouse Community Primary School

Document Control

Version	*Date*	*Author*	*Comments*
Issue 1	**September 2024**	**KW**	*New policy*
	November 2025	**KW**	*Readopted with changes to agreements to align to the Acceptable ICT policy*

Owner: DPO
Approver: Trust Board
Statutory Policy: Yes
Review Cycle: Annual
Approval date: 18th December 2025

Policy Contents

1. Introduction and Aims

The Children's Endeavour Trust (collectively referred as "CET" or "Trust") and its schools are committed to protecting the rights and freedom of all individuals in relation to the processing of their data.

This policy aims to:

- Ensure that the Trust and schools have robust processes in place to ensure the online safety of pupils, staff, volunteers, governors and trustees.
- Identify and support groups of pupils 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.

The 4 key categories of risk

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

A. **Content** - being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

B. **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

C. **Conduct** - personal online behavior 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; and

D. **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools

- Preventing and tackling bulling and cyber-bulling, advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Reference 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 pupils' 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 and complies with our funding agreement and articles of association.

3. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust:

CEO and Trust Board

The CEO and Trust Board have overall responsibility for the approval and monitoring of this policy and holding the headteachers to account for its implementation.

The IT Trust Development Lead

The Trust IT Development Lead will keep under review the DfE filtering and monitoring standards, and discuss with Trust Staff, School Leaders, DSLs, IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Trust IT Development Lead is responsible for working with Headteachers in:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 IT staff or IT providers keep systems 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 on a regular basis
- Ensure that IT staff or IT providers block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Supporting Headteachers and DSLs when required
- Assisting schools with any incidents of cyber-bullying, in line with their school's behavior policy
- Assisting schools when required with online safety incidents, in line with this policy

This list is not intended to be exhaustive.

School Governors

All governors will:

- Ensure they have read this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).
- Checking that online safety is a running and interrelated theme within the whole-school 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.

This list is not intended to be exhaustive.

School Headteachers

Headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout their school.

Headteachers will:

- 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.
- Make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- 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).
- Ensure children are taught how to keep themselves and others safe, including keeping safe online.

- Ensure their school has appropriate filtering and monitoring systems in place on school devices and school networks and regularly review their effectiveness.

This list is not intended to be exhaustive.

Designated Safeguarding Leads (DSLs)

Details of the school's DSL and alternative DSLs are set out in our Child Protection and Safeguarding Policy.

DSLs take lead responsibility for online safety in schools, in particular:

- Supporting the Headteachers in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with Headteachers and Local Governing Bodies to ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Trust IT Development Lead to make sure the appropriate systems and processes are in place
- Working with their Headteacher, the Trust IT Development Lead, ICT staff or providers 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 and safeguarding policy
- Ensuring that any online safety incidents are logged, and dealt with appropriately in line with this policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to their Headteacher and Local Governing Body.
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing 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.

This list is not intended to be exhaustive.

Teaching, Support Staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- All school staff are expected to read, understand and abide by the Acceptable Use Agreement (Appendix 3).

This must be done by acknowledging that they have read and understood appendix 3, as part of this policy, on our HR Access System or on I AM Compliant.

- Monitoring pupils use of digital technologies such as iPads, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Knowing who the DSL and Alternative DSLs are
- Understanding that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting via CPOMS or MyConcern
- Working with the DSL to ensure that any online safety incidents are logged
- 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'*

This list is not intended to be exhaustive.

Pupils

Pupils are required to abide by the Acceptable Use Agreement for Pupils (appendix 2).

Parent and carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Parents/carers will be encouraged to support the Trust in promoting good online safety practices

Parents/carers 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 (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- UK Safer Internet Centre
- Childnet

Visitors and members of the community

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 (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

- Relationships and sex education and health education in secondary schools

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.

5. Educating parents about online safety

All of the schools within the Trust will take every opportunity to raise parents' awareness of internet safety, through parents' evenings, newsletters, letters and their school's website.

The school will let parents/carers know:

1. 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
2. What systems the school uses to filter and monitor online use

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.

6. 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.

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.

Our schools 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 (see section 11 for more detail).

All the schools within the Trust will post information on cyber-bullying on their website and school newsletters, so parents 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 their 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 incidents 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

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

1. Poses a risk to staff or pupils, and/or
2. Is identified in the school rules as a banned item for which a search can be carried out, and/or
3. 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 or DSL.
- 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 co-operation

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 staff member in conjunction with 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/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 (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 screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The School Behaviour Policy

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

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help pupils 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.
The Trust and schools will treat any use of AI to bully pupils in line with their school's behaviour policy. 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 their school.

7. Acceptable use of the internet in school

All pupils, parents/carers, volunteers and governors are required to sign an agreement regarding the acceptable use of the school's ICT systems (AUP) and the internet.

All staff are required to acknowledge that they have read, understood and will abide by the Acceptable Use Agreement (appendix 3) on the Trust's HR Access System (or on I AM Compliant).

Please view our Acceptable Use Agreements in appendices 1 to 3. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

8. Pupils using mobile devices in school

Pupils may bring their mobile devices into school, but are not permitted to use them on site, or during the school day. These devices must be switched off during school hours.
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.

9. 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 using the three random word technique recommended by the National Cyber Security Centre for more information, please see the Trust's Password Policy
- To include a combination of upper and lower-case letters, numbers and special characters
- Ensuring their laptop hard drive is encrypted - this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Only encrypted memory storage devices can be used, the Trust generally discourages the use of these devices
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Make sure the schools IT staff or provider has installed anti-virus and spyware
- It is your responsibility to keep the anti-virus up to date
- Employees are allowed to use personal devices to complete two-factor authentication (2FA) requirements
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use agreement, as set out in appendix 3. See the Trust website for the full AUP
- 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 IT staff or provider.

10. How each school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school may sanction pupils, as per school Behaviour Policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Examples of misuse include (this list is not intended to be exhaustive):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the schools' policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school(s), or risks bringing the school into disrepute

- Sharing confidential information about the school(s), other pupils, or other members of the school communities
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the schools' ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

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/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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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.

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 the risks up
    - 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 deputy/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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. If you have a concern please report using your school's reporting platform (for example CPOMS or MyConcern).
This policy will be reviewed annually and shared with the CEO and Trust Board.

13. Links with other policies

This Online Safety policy is link to our:
- Child Protection and Safeguarding Policy
- Each School's Behaviour Policy
- Password Policy
- Data Protection Policy
- Privacy Notices
- Acceptable Use policy

Appendix 1:

Acceptable Use of The Internet: Agreement for Parents and Carers	
Name of parent/carer: **Name of pupil:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Arbor app • Email and Text groups for parents (for school announcements and information) • Tapestry Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way • Use private groups, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**
Print name:	

Appendix 2:

Acceptable Use of The School's ICT Facilities and Internet: Agreement for Pupils and Parents/Carers

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me)
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Share my password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit if as my own work.
- Use my phone or smart watch during school hours

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**
Print Name (pupil):	

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 3:

Acceptable Use of The School's ICT Facilities and The Internet:
Agreement for Staff, Governors, Volunteers and Visitors

Name:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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
- 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
- Use my mobile phone or smart watch when in class with pupils

Promote any private business, unless that business is directly related to the school

I understand 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 staff/provider 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.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Staff must acknowledge that they have read and understood this, as part of this policy, on our HR Access System or on I AM Compliant.

Staff/Governors/volunteers/visitors must sign below:

Signed (staff/governor/volunteer/visitor):	**Date:**

Print name (staff/governor/volunteer/visitor):