Scholes (Elmet) Primary
St James' CE Primary
Moortown Primary

Policy: Online safety

Date: September 2023

Introduction

Throughout their time at school, pupils will use technology, both on and offline, to support their learning. This will take many forms. For example, logging in to a learning platform; conducting research using a search engine; creating, editing, saving digital content. At times, children will be using technology independently and at other times with a partner or as part of a group. This policy explains how we will keep children and staff safe whilst online.

1. Aims

Sphere Federation schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **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
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (eg consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **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 (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 head of federations 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 pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the head of federation to account for its implementation.

The governing board 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.

The governing board will also 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.

The governing board will 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).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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 governor who oversees online safety is the Safeguarding Governor.

All governors will:

- ensure 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 (appendix 3)
- 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

3.2 The head of federation

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

3.3 The designated safeguarding lead (DSL)

Details of each schools' DSL and safeguarding team are set out in our Safeguarding and Child Protection Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- supporting the head of federation in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the head of federation and governing board to review this policy annually and 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 ICT manager to make sure the appropriate systems and processes are in place
- working with the head of federation, 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 Safeguarding and 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
- 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.

3.4 The ICT manager

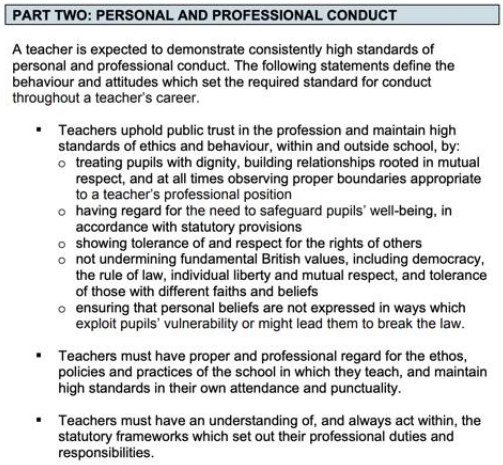
The ICT manager is responsible for:

- 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 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 on a on an appropriate basis eg filtering on a weekly basis, checks on firewall weekly, checks on server and data back-ups fortnightly, checks on Windows monthly
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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 dealt with appropriately in line with the Positive Relationships Policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

Whilst written in the context of just teachers, Part 2 of the Teachers' Standards are relevant for all staff in the context of online safety.



PART TWO: PERSONAL AND PROFESSIONAL CONDUCT

A teacher is expected to demonstrate consistently high standards of personal and professional conduct. The following statements define the behaviour and attitudes which set the required standard for conduct throughout a teacher's career.

- Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:
  - treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position
  - having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions
  - showing tolerance of and respect for the rights of others
  - not undermining fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs
  - ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law.
- Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach, and maintain high standards in their own attendance and punctuality.
- Teachers must have an understanding of, and always act within, the statutory frameworks which set out their professional duties and responsibilities.

All staff, including contractors, 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 (Appendix 3), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1, Appendix 2)
- knowing 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 alerting the DSL / Head of School
- following the correct procedures by contact ICT support if they need to bypass the filtering and monitoring systems for educational purposes
- working with the DSL to ensure that any online safety incidents are logged (using CPOMS) 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's Positive Relationships 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.

3.6 Parents/carers

Parents and carers are expected to:

- notify a member of staff or the Head of School 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 (Appendix 1, Appendix 2)

Parents and 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

3.7 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 are expected to agree to the terms on acceptable use (Appendix 3).

4. Educating pupils about online safety

Pupils are taught about online safety as part of the curriculum. The text below is taken from the National Curriculum Computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach Relationships education and health education in primary schools

In **Key Stage 1**, pupils are 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** are 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 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 is also covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and disabilities (SEND).

5. Educating parents and carers about online safety

Sphere Federation schools raise parents' and carers' awareness of internet safety in various online communications, such as Friday's weekly message, and dedicated pages on the school websites (see below):

- Scholes (Elmet) Primary: https://www.scholeselmet.leeds.sch.uk/learn-more/online-safety/
- Moortown Primary: https://www.moortown.leeds.sch.uk/learn-more/online-safety/
- St James' CE Primary: https://www.stjameswetherby.leeds.sch.uk/learn-more/online-safety/

Frequent references are made to online safety in the weekly messages each Friday (published online, with a Twitter and Facebook alert, and emailed to parents). Parents and carers are strongly advised to engage with the content.

This policy is available to parents and carers on the Sphere Federation schools' websites. A paper copy can be provided on request.

Online safety is also covered in scheduled parent-teacher communications: Learning Updates and/or parent-teacher meetings.

Systems are filtered and monitored by several different means including 'Impero' and 'Netsweeper'; these are managed by Adept in consultation with Head of Federation, Head of Schools and IT Lead.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School (who is also the designated safeguarding lead).

Similarly, concerns or queries about this policy can be raised with the Head of School or the Head of Federation.

6. Cyber-bullying

6.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Positive Relationships policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We 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.

We 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 (referred to as Living and Learning), 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).

We also communicate information 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, we follow the processes set out in the Positive Relationships policy. Where illegal, inappropriate or harmful material has been spread among pupils, we 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.

6.3 Examining electronic devices

The Head of Federation, Head of School (and Deputy Head of School at Scholes (Elmet) Primary and Moortown Primary) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- poses a risk to staff or pupils
- is identified in policies as a banned item for which a search can be carried out
- 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 other Sphere Federation senior leaders or the LA
- 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
- 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 Head of Federation or Head of School 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
- 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 searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- our Positive Relationships Policy

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

6.4 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.

Sphere Federation 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.

Sphere Federation schools will treat any use of AI to bully pupils in line with our Positive Relationships 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 the Sphere Federation.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1-3). Visitors are 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 pupils, staff, volunteers, governors 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 agreements in Appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils are discouraged from bringing mobile devices into school. However, if they do, the device must be switched off and handed over to staff at the start of the school day.

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

9. Staff using work devices outside school

Refer to Section 3.5 for staff roles and responsibilities; these apply to the use of work devices both in school and outside.

All staff members 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 (eg asterisk or currency symbol)

- Ensuring their 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
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 3.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager or their Head of School.

10. How the school responds to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we follow the procedures set out in our Positive Relationships Policy. 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 Leeds Disciplinary Policy and Procedure for School Based Staff. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

We will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the Local Authority Designated Officer (LADO) and/or the police.

11. Training

New staff members receive comprehensive information and policies, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

Staff members 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, staff are 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 also helps 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 other members of the safeguarding team undertake child protection and safeguarding training, which will include online safety, at least every two years. They also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors have access to training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection Policy.

12. Monitoring arrangements

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

This policy is reviewed every year by the Senior Leadership Team (or earlier if required). At every review, the policy is shared with the governing board. The review (such as the one available here) is supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Positive Relationships Policy
- Disciplinary Policy and Procedure (staff)
- Data Protection Policy and privacy notices
- Complaints Policy
- ICT and Internet Acceptable Use Policies

This list is not intended to be exhaustive.

Being online – acceptable use agreement

Name of pupil:

When I use the 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 select 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.

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

Parent/carer agreement:

Please read the following and sign to show your agreement. If we don't receive your signed agreement, your child may not have access to electronic devices that support learning.

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.
I will discuss these points with my child.
I will encourage the same safe practice when my child is at home.

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

Being online: Acceptable use agreement

Name of pupil:

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

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

- Always use the 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 usernames 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 trusted adult) immediately if I find any material which might upset, distress or harm me or others.
- Only create, link to or post material that is appropriate and respectful.
- Always log off or shut down a computer when I'm finished working on it.

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless a teacher has 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 in to the school's network or other systems 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:

- I will hand it in at the start of every school day and collect it at the end.

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

Signed (pupil):	**Date:**

Parent/carer's agreement:
Please read the following and sign to show your agreement. If we don't receive your signed agreement, your child may not have access to electronic devices that support learning in 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 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.
I will encourage the same safe practice when my child is at home.

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

Online safety policy: Appendix 3
Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors

Being online: Acceptable use agreement

Adults in school have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in this policy.

Name of staff member / governor / volunteer / visitor:	

- I have read and understood Sphere Federation's full Online Safety Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils.
- I understand that this Acceptable Use Agreement and the Online Safety Policy are important parts of Sphere Federation safeguarding procedures.
- I understand that breach of this Acceptable Use Agreement and/or of the full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), *I will*:

- Abide by the responsibilities listed for my role (Section 3 in the Online Safety Policy) and understand and support the commitments made by pupils and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with Sphere Federation procedures.
- Uphold my online reputation, my professional reputation and that of the school, and I will do nothing to impair either.
- 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.
- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Prepare and check all online source and resources before using.
- Support the Sphere Federation whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or the Head of Federation (if by an adult).
- Inform Designated Safeguarding Lead if a pupil tells 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.
- Record online safety concerns in the same way as any safeguarding incident and report in accordance with school procedures.
- Whenever overseeing the use of technology, I will supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data law.
- Always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- As a role model, promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media.
- Adhere to all provisions of the Sphere Federation Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for.

- Protect my passwords/logins and other access; and will immediately change passwords and notify the Head of School if I suspect a breach.
- Look after devices loaned to me.
- Notify the Designated Safeguarding Lead and/or Head of School if policy does not reflect practice in your school and I will follow escalation procedures if concerns are not promptly acted upon.
- Notify the Designated Safeguarding Lead of new trends and issues that I am aware of before they become a problem.
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, and make the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

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).
- Support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school; I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- 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.
- I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
- Take photographs of pupils without checking with teachers first.
- Use my phone or other electronic device to capture images or other content that is directly related to school (eg photographs of pupils, contact details).
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Attempt to bypass security or monitoring.
- 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.
- Contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways; I will report any breach of this by others or attempts by pupils to do the same to the Designated Safeguarding Lead and/or Head of Federation.

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

Online safety training needs – self-audit for staff

Name of staff member/volunteer:	**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?	
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?	