# DAYSPRING TRUST – NOW NORTHERN LIGHTS LEARNING TRUST

## Online Safety Policy

Northern Lights Learning Trust (NLLT) have adopted all policies pertaining to Dayspring Trust – Ian Ramsey CE Academy and Venerable Bede CE Academy – from 1 February 2023 and will be reviewed in due course.

Ratified by: Executive Headteacher
Date of review: Autumn Term 2022
Date of next review: Autumn Term 2025

The Dayspring Trust aims to serve its community by providing an education of the highest quality within the context of Christian faith and practice. It encourages an understanding of the meaning and significance of faith and promotes Christian values through the experience it offers to all its pupils. We believe that our Christian values spring from the two great commandments, 'Love God and love your neighbour'. We seek to live this out through the power of the Holy Spirit. St Paul reminds us in Galatians 5:22-23 that the fruit of the Spirit is 'Love, joy, peace, patience, kindness, goodness, faithfulness, gentleness and self-control'. These are also underpinned by the Old Testament injunction to 'Do justly, love mercy and walk humbly with our God', Micah 6:8. These values rooted in the Christian Faith come as a package and we aim to embed them in the life of our academies in a worked-out way. We recognise that at times we may highlight values to bring them into greater prominence within our academies and these are currently the five values of Forgiveness, Hope, Joy, Perseverance and Wisdom. We believe these values to be in accordance with British values springing from our Judeo-Christian roots. Collective worship will play a major and vital part in assisting with this process of embedding these values in the life of our academies.

The Multi Academy Trust Members and Directors are aware of their responsibilities in law and are committed to the provision of an excellent education within its academies in accordance with our Anglican foundation. This is embraced in our Dayspring Trust vision statement:

- **Forge a supportive and challenging family of academies**
- **Provide excellent education within a strong Christian community**
- **Resource our pupils for wise and generous living**

In addition, each academy also has its own distinctive mission statement, flowing out from the vision statement of the Dayspring Trust.

**At Ian Ramsey CE Academy:**

'Together to learn, to grow, to serve.'

This is embodied in scripture:

*'Each of you should use whatever gifts you have received to serve others, as faithful stewards of God's grace in its various forms.' 1 Peter 4:10*

**At Venerable Bede CE Academy:**

'Soar to the heights together.'

This is embodied in scripture:

*'But those who hope in the Lord will renew their strength. They will soar on wings like eagles; they will run and not grow weary; they will walk and not be faint.' Isaiah 40:31*

This policy has been developed to take into consideration our ethos as well as local and national policy and guidance.

# Contents

Relevant staff

Safeguarding Trustee:
Mark Stouph
Email: Katrina.Durrans@venerablebede.co.uk

Head Teacher (Venerable Bede CE Academy):
Mr D Airey
Email: Tracy.Gray@venerablebede.co.uk

Designated Safeguarding Lead (Venerable Bede CE Academy):
Mrs S Holt
Email: Sally.Holt@venerablebede.co.uk

## 1. Aims

The Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and Trust Directors.
- 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 (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

## 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 online-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has

given teachers stronger powers to tackle online-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 considers the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

# 3. Roles and responsibilities

## 3.1 The MAT Board

The MAT Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The MAT board 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).

The Director who oversees online safety is the Safeguarding Director.

All Directors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 3).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. This responsibility may be delegated to the Safeguarding Officer to implement.

## 3.3 The Designated Safeguarding Lead

Details of the Academy's DSL [and deputy DSLs] are set out in our child protection policy as well as relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy.
- 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 Academy's 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 online-bullying are logged and dealt with appropriately in line with the Academy's 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 the Academy to the Headteacher and/or MAT board.

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, 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 the Academy, including terrorist and extremist material
- Ensuring that the Academy'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 Academy's ICT systems on a regular basis, depending on system requirements.
- 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 online-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

## 3.5 All 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.
- 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 (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of online-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.

## 3.6 Parents

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 Academy's ICT systems and internet (appendices 1 and 2).

Parents 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
- Healthy relationships – Disrespect Nobody

## 3.7 Visitors and members of the community

Visitors and members of the community who use the Academy'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, taken from the guidance on relationships education, relationships and sex education (RSE) and health education and Relationships and sex education and health education for secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

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

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared, and used online.
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

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. Curriculum

Online safety is embedded within our curriculum. The Trust provides a comprehensive curriculum for online safety which enables pupils to become informed, safe, and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

In all curriculum areas, online safety is a focus and staff are expected to reinforce online safety messages in the use of ICT. In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use. Where pupils are allowed to freely search the internet, e.g., using search engines, staff are expected to be vigilant in monitoring the content of the websites the young people visit.

It is accepted that, from time to time, and for good educational reasons, pupils may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Manager temporarily removes those sites from the filtered list for the period of study. Any request to do so must be auditable, with clear reasons for the need. Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information, they are also taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are explicitly taught how to remain safe whilst accessing the internet.

**The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may, as part of a pupil's digital footprint, remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term, indeed, there are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The Trust informs and educates users about the following risks to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. Pupils are taught to recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Staff are allowed to take digital/video images to support educational aims.
- Such images must only be taken on Trust equipment; equipment owned by staff members must not be used.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the Academies' websites or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

It is necessary for pupils to develop skills of critical awareness, digital resilience, and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic, and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g., regulated screen time and diverse online activity.
- Learning how to develop a positive online reputation and enhance future opportunities e.g., in relationships and employment.
- Developing critical thinking skills in relation to online content e.g., recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e., users may not be who they say they are and may have ulterior motives).
- Understanding the dangers of giving out personal details online (e.g., full name, address, mobile/home phone numbers, school details, email address) and the importance of maintaining maximum privacy online.
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.

- Understanding the permanency of all online postings and conversations.
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation, and images.
- What constitutes online-bullying, how to avoid it, the impact it has and how to access help.

## 6. Educating parents about online safety

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

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

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

## 7. Online-bullying

### 7.1 Definition

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

### 7.2 Preventing and addressing online-bullying

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

The Academy will actively discuss online-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss online-bullying with pupils.

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

All staff, directors, and volunteers (where appropriate) receive training on online-bullying, its impact, and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The Academy also sends information on online-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 online-bullying, the Academy will follow the processes set out in the Academy's behaviour policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the Academy will use all reasonable endeavours to ensure the incident is contained.

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

### 7.3 Examining electronic devices

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

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

- Cause harm, and/or

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

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

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

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

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

## 8. Acceptable use of the internet in the Academy

All pupils, parents, staff, volunteers, and directors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

Use of the Academy'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, directors, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices 1, 2.

## 9. Pupils using mobile devices in the Academy

Pupils may bring mobile devices with them into the Academy, but they should be switched off and not used in school.

Any breach by a pupil may trigger disciplinary action in line with the Academy's behaviour policy, which may result in the confiscation of their device.

## 10. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g., asterisk or currency symbol).
- 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 install the latest updates.

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

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 Academy's ICT Manager.

## 11. How the Academy will respond to issues of misuse

Where a pupil misuses the Academy's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 Academy'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 Academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including online-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 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 DSLs] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Directors 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.

## 13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL. Every review, the policy will be shared with the MAT Board. The review (such as the one available here) will be 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.

## 14. Links with other policies

This online safety policy is linked to our:

- Child Protection policy
- Child on Child Abuse policy
- Behaviour, Discipline, Suspension and Permanent Exclusion policy
- Disciplinary policy
- GDPR Data Protection policy & Protection of Biometric Data
- Complaints policy
- IT and Communications Systems policy

# Appendix 1: Acceptable use agreement (pupils and parents/carers)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| **Name of pupil:** | |
| **I will read and follow the rules in the acceptable use agreement policy**<br>**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**<br>• Always use the school's ICT systems and the internet responsibly and for educational purposes only<br>• Only use them when a member of staff is present, or with a member of staff's permission<br>• Keep my username and passwords safe and not share these with others<br>• 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<br>• Tell a member of staff immediately if I find any material which might upset, distress or harm me or others<br>• Always log off or shut down a computer when I'm finished working on it<br>**I will not:**<br>• Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless a member of staff has expressly allowed this as part of a learning activity<br>• Open any attachments in emails, or follow any links in emails, without first checking with a member of staff<br>• Use any inappropriate language when communicating online, including in emails<br>• Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate<br>• Log in to the school's network using someone else's details<br>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision<br>**If I bring a personal mobile phone or other personal electronic device into school:**<br>• I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a member of staff's permission<br>• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online<br>**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:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

# Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| **When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**<br>• 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)<br>• Use them in any way which could harm the school's reputation<br>• Access social networking sites or chat rooms<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>• Share my password with others or log in to the school's network using someone else's details<br>• Take photographs of pupils without checking with teachers first<br>• Share confidential information about the school, its pupils or staff, or other members of the community<br>• Access, modify or share data I'm not authorised to access, modify or share<br>• Promote private businesses, unless that business is directly related to the school | |
| I have read and understood the school's Online Safety policy.<br>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.<br>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>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.<br>I will 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.<br>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 3: online safety training needs – self audit for staff

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **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 online-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |

## Appendix 4: online safety incident report log

| ONLINE SAFETY INCIDENT LOG | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |