

# NEW FOREST CARE EDUCATION

## Online Safety Policy

## Contents

|   |    |
|---|----|
| 1. Aims .....   | 3  |
| 2. Legislation and guidance .....   | 3  |
| 3. Roles and responsibilities .....   | 4  |
| 4. Educating students about online safety .....   | 7  |
| 5. Educating parents about online safety .....  | 8  |
| 6. Cyber-bullying .....   | 8  |
| 7. Acceptable use of the internet in school .....   | 10 |
| 8. Students using mobile devices in school .....  | 10 |
| 9. Staff using work devices outside school .....  | 11 |
| 10. How the school will respond to issues of misuse .....                                 | 11 |
| 11. Training .....  | 11 |
| 12. Monitoring arrangements .....   | 12 |
| 13. Links with other policies .....   | 12 |
| Appendix 1: KS2, KS3 and KS4 acceptable use agreement (students and parents/carers) ..... | 14 |
| Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) .....    | 16 |
| Appendix 3: online safety training needs – self audit for staff .....                     | 17 |

**This policy applies to all areas of New Forest Care Education’s business, including Registered Independent Schools, Alternative Provisions, Farms, Post-16 and all other Educational Services.**

## 1. Aims

New Forest Care Education aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students 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/alternative education 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, antisemitism, 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 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 headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department’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 students’ 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.

## 3. Roles and responsibilities

### 3.1 The Governing Board/Directors of Education

The Governing Board/Director of Education has overall responsibility for monitoring this policy and holding the Headteachers and Head of Alternative Education to account for its implementation.

The Governing Board/Director of Education 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/Director of Education 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/Director of Education 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/Director of Education should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Board/Director of Education must ensure the Schools/Alternative Education Provisions has appropriate filtering and monitoring systems in place on devices and networks, and will regularly review their effectiveness. The board/Director will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support 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.

All Governors/Directors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of NFCEs 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 Alternative Education 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 students 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 Headteacher/Head of Alternative Education

The Headteacher/Head of Alternative Education is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school/alternative education provision.

### 3.3 The Designated Safeguarding Lead

Details of the school's/Alternative Education designated safeguarding lead (DSL), deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher/ head of alternative education in ensuring that staff understand this policy and that it is being implemented consistently
- Working with the headteacher and Governing Board/Director of Education 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 devices and networks in all NFCE's education provisions and schools
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher or Head of Alternative Education, 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 NFCE 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 Support Manager**

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on all devices and networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school or accessing and Alternative Education provision, including terrorist and extremist material
- Ensuring that the 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 ICT systems on a regular
- 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 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 ICT systems and the internet (appendix 3), and ensuring that students follow the terms on acceptable use (appendices 1 and 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 speaking to a DSL or submitting an IT Support Ticket
- Following the correct procedures by seeking permission from SLT and submitting an IT Support Ticket 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 (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 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 ICT systems and internet (appendices 1)

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 factsheet - [Childnet International](#)

### **3.7 Visitors and members of the community**

Visitors and members of the community who use the 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 students about online safety

Students will be taught about online safety as part of the curriculum in all NFCEs' schools. Alternative Education Provisions may undertake this as part of the curriculum:

Students in **Key Stage 2** 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
- Students 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**, students 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

In **Key Stage 3**, students 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

Students 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**, students 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 that 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)

## 5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings in NFCE Schools.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

## 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 school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

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



All NFCE Schools and Alternative Education Provisions will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors/teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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 students, as part of safeguarding training (see section 11 for more detail).

All NFCE Schools and Alternative Provisions send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. Parents are also provided with free online training on cyber-bullying and online safety.

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

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

### **6.3 Examining electronic devices**

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

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a member of SLT.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student'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 [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

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

The Head of Alternative Education will follow these procedures, in conjunction with Local Education Authority, named School or parent.

## 7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the NFCE's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the terms on acceptable use if relevant.

Use of the NFCEs' 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 students, staff, volunteers, governors 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 and 3.

## 8. Students using mobile devices in school

Students may bring mobile devices on to NFCEs Education sites if agreed between the lead staff and parents/carers. The device should be handed in to the school office for safekeeping during the school day.

Alternative Education Provisions will agree an individual plan for students. Students are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Unless specifically agreed with the Senior Leadership Team/Teacher and student, for example: use within an ICT lesson.

Any use of mobile devices by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student 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 of working hours or off-site**

Staff members using a work device outside of working hours or off-site must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Only encrypted USB devices provided by New Forest Care Ltd should be used to store student or staff data.

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

Work devices must be used solely for work activities.

## **10. How the school AND Alternative education Provision will respond to issues of misuse**

Where a student misuses the NFCE'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 NFCE'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 for New Forest Care Ltd. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

New Forest Care Ltd. will consider whether incidents which it suspects 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 (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Headteacher, Head of Alternative Provision and Director of Education. At every review, the policy will be shared with the governing board.

## **13. Links with other policies**

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices

- Complaints procedure
- ICT and internet acceptable use policy

## Appendix 1: KS2, KS3 & KS4 acceptable use agreement (students and parents/carers)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

**Name of student:**

**I will read and follow the rules in this acceptable use policy before I access the school's ICT Systems and understand**

#### **Equipment**

- Do not install, attempt to install, or store programs of any type on the computers without permission.
- Do not damage, disable, harm the operation of computers, or intentionally waste resources.
- Do not open files brought in on removable media (USB drives etc.).
- Do not connect mobile equipment to the network.
- Do not eat or drink near computer equipment.

#### **Security and privacy**

- Do not disclose your password to others. Never tell anyone you meet on the internet: your home address, your telephone number, any details about the school, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends, or insults others. Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas will be treated like school desks. Staff may review files and communications to ensure that users are using the system responsibly.

#### **Internet**

- The internet should only be used for study or for school authorised/supervised activities.
- Do not use the internet to obtain, download, send, print, display, or otherwise transmit or gain access to materials which are unlawful, obscene, or abusive.
- Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the internet.
- Never arrange to meet anyone via the internet. People you contact online are not always who they seem.

#### **Email**

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing, or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy information and software on the computers.
- The sending or receiving of emails containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any content of a violent, dangerous, racist, or inappropriate nature. Always report such messages to a member of staff.

**I agree that the school will monitor the websites I visit, emails I send and files I create/store and that there will be consequences if I don't follow the rules.**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

**Signed (student):**

**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 students 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 NCFES' 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:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of students without checking with teachers first
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

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

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT Support know if a student 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 students 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   |   |
|--|---|
| <b>Name of staff member/volunteer:</b>   | <b>Date:</b>                              |
| <b>Question</b>  | <b>Yes/No (add comments if necessary)</b> |
| Do you know the name of the person who has lead responsibility for online safety in school?                |   |
| Do you know what you must do if a student 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 students 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?                    |   |