Dalestorth Primary and Nursery School

Online Safety Policy September 2025

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 7
6. Cyber-bullying 8
7. Acceptable use of the internet in school 10
8. Pupils using mobile devices in school 10
9. Staff using work devices outside school 10
10. How the school will respond to issues of misuse 10
11. Training 11
12. Monitoring arrangements 11
13. Links with other policies 11
Appendix 1: Home School Agreement 13
Appendix 2: Acceptable use agreement (all pupils) 14
Appendix 3: Policy for responsible e-mail, network and Internet use for staff 15
Appendix 4: Laptop code of conduct 16
Appendix 5: Online Safety Training Audit 17

1. Aims

Our school aims 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, misinformation, disinformation (including fake news), conspiracy theories, 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's) 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 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.

Maintained schools and academies that follow the National Curriculum insert:

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

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher 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 aall 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 Mrs Wain.

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 headteacher

The headteacher 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

Details of the school's designated safeguarding lead (DSL) 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 school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher 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 Technical staff to make sure the appropriate systems and processes are in place
- Working with the headteacher, Technical staff and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMs 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
- 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 Technical staff

The technical staff are 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 fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on 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 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)
- 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 reporting these to ATOM IT.
- Following the correct procedures by contacting the technical staff 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 on 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 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/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- 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 will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

In Key Stage (KS) 1, pupils will be taught to:

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

Pupils in Key Stage (KS) 2 will be taught to:

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

By the end of primary school, pupils will know:
· That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
· The benefits of rationing time spent online, the risks of excessive use, and the impact on wellbeing
· Why social media, computer games and online gaming have age restrictions
· How information, including from search engines, is ranked, selected and targeted

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

The school 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.

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 and/or the DSL.

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

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 1 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 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 school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes as part of ICT sessions.

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

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

The school also sends information/leaflets on cyber-bullying to parents/carers so 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, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will 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

- If content is contained on learner's personal devices they will be managed in accordance with the Department for Educations 'search, screening and confiscation' advice. The head teacher, and any member of staff authorised to do so by the head teacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

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

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to teacher in partnership with the DSL 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. (This must always be followed without exception)

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 good relationships and behaviour 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.

Dalestorth Primary and Nursery School 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.

Dalestorth Primary and Nursery School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

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 school.
· Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 to 3). Visitors will be 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 to 3.

8. Pupils using mobile devices in school

Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.

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

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

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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 by always installing the latest updates

Staff members must not use the device in any way that would violate the school'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 technical staff.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour 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 the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that 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 the DSL 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

Staff will log behaviour and safeguarding issues related to online safety. An incident report log can be found on CPOMs.

This policy will be reviewed every year by the Computing Lead. At every review, the policy will be shared with the governing board. This review will be supported by an annual risk assessment that considers and reflects the risks pupils face online.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Our good relationships and behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices

- Complaints procedure
- ICT and internet acceptable use policy

POLICY REVIEW

- This policy is to be reviewed every year
- Policy written by C Wood September 2023
- Policy due to reviewed: September 2027

Dalestorth Primary and Nursery School
Home School Agreement

Our Vision
All of our children will be successful because they are always at the centre of that we do.

Our Aims
Our children will be kept safe and we will support our families at all times.
Our children will be provided with a high-quality curriculum which consistently excites and challenges them and enables them to build a wide body of knowledge.
Our children can apply and reason about the body of knowledge they develop over time.
Our children will be the best version of themselves that they can be by the end of Year 6.
Our children will be kind and caring to adults and other children at all times.
Our children will understand the value of forming positive relationships with both children and adults.
Our children will become brave and resilient individuals who are able to cope and learn from difficulties and change in their lives.
Our children will grow into excellent friends who are trustworthy and respectful of others.
Our children learn about their community and play an active role in it.

Our Five Busy Bee Values
Be honest
Be kind
Be brave
Be you
Be a friend

The school will:
Care for and respect each child as an individual.
Encourage high expectations and pride in achievement in all areas.
Provide opportunities for pupils to develop their potential in all areas.
Inform parents of the progress and welfare of their child.
Provide and monitor homework which is appropriate to the child's needs.
Provide a safe, happy and orderly environment in which to work and play.
Listen to parents' views and concerns.
Seek the support of parents if a child's behaviour choices noticeably change for the worse.
Investigate all allegations of bullying.

Families will:
Support the schools in its aims and values.
Ensure their child's regular and punctual attendance.
Avoid taking holidays in term time.
Notify the school early on the first day of the reason for their child's absence.
Support the school's policy for Good Relationships and Behaviour.
Work with the school to eliminate all forms of bullying.
Support the child in the school work they are expected to do at home.
Listen to their child read at least 3 times a week.
Tell the school about any circumstances which may affect their child.
Attend parents' evenings and discussions about their child's progress.
Keep up to date with school events through the school newsletter, Class Dojo, the website and letters sent home.
Ensure their child wears the correct school uniform and has the correct PE kit.
Speak to the class teacher in the first instance if they have a concern and use the appropriate escalation policy to achieve a resolution to that concern, rather than via other means (e.g. social media).
Give permission for my child to use the school's ICT systems and the internet under staff supervision and ensure they understand and follow the rules set out in the school's Acceptable Use Agreement.

Pupils will:
Arrive at school on time.
Bring the correct equipment I need each day.
Wear the correct school uniform and have the correct P.E.kit.
Follow the 5 Busy Bee Dalestorth Values.
Follow the school rules and behaviour guidelines.
Complete all my class and homework on time.
Always try my best and work hard.
Tell my teacher or parent/carer if I am worried about my school work or the behaviour choices of others
Look after the school building, equipment and school environment.
Use the school's computers and internet only for learning and with a teacher's permission.
Tell a teacher straight away if I see anything online that upsets or worries me.
Never share my personal information, like my name or phone number, without permission from a teacher or parent.

……

We understand and accept the school's expectations outlined in this home/school agreement.
Signed…… Parent/Carer …….. Pupil

Dalestorth Primary and Nursery School
Online Safety Agreement for Pupils

When I use the school's ICT systems (like computers, tablets, or laptops) and go on the internet in school, I will:

- Ask a teacher or adult before using them.
- Only use websites, apps, or programs that a teacher or adult has told me I can use.
- Use the school's ICT systems responsibly and for schoolwork and learning.
- Be kind and respectful to others online and not use rude or hurtful language.
- Look after school ICT equipment and tell a teacher straight away if something is broken or not working properly.
- Always log off or shut down a computer/device when I have finished using it.

I will keep myself and others safe by:

- Keeping my usernames and passwords private and not sharing them with anyone.
- Trying hard to remember my username and password.
- Never give out personal information (like my full name, address or phone number) without a teacher's or parent/carer's permission.
- Telling a teacher (or another sensible adult) immediately if: - I select a website by mistake - I
- receive messages from people I don't know - I find something online that upsets or worries me, or that could harm me or others.
- Not arranging to meet anyone offline that I have spoken to online, without my parent/carer and a trusted adult knowing and being with me.

I will not:

- Go onto inappropriate websites (for example, social networking sites, chat rooms, gaming sites) unless my teacher has allowed it as part of my learning.
- Open email attachments or follow links without checking with a teacher first.
- Create, share, or link to anything that is rude, unkind, offensive, or inappropriate.
- Log in using someone else's details.

If I bring a personal mobile phone or other electronic device into school (only if allowed):

- I will not use it during lessons, clubs, or school activities without my teacher's permission.
- I will use it responsibly, and I will not access inappropriate websites or use unkind or inappropriate language.

I understand that:

- The school will monitor the websites I visit and my use of ICT systems.

……

We understand and accept the school's expectations outlined in this Online Safety agreement.

Signed…….. Parent/Carer …….. Pupil

Policy for responsible e-mail, network and Internet use for Dalestorth Primary and Nursery School

1. I will use all ICT equipment issued to me in an appropriate way. I will not:

- Access offensive website or download offensive material.
- Make excessive personal use of the Internet or e-mail.
- Copy information from the Internet that is copyright or without the owner's permission.
- Place inappropriate material onto the Internet.
- Will not send e-mails that are offensive or otherwise inappropriate.
- Disregarded my responsibilities for security and confidentiality.
- Download files that will adversely affect the security of the laptop and school network.
- Access the files of others or attempt to alter the computer settings.
- Update web pages etc. or use pictures or text that can identify the school, without the permission of the Head Teacher/ Deputy Head.
- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Dalestorth Primary and Nursery School.

2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the ICT School's Technician as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working. ·
5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Head Teacher/ Deputy Head and register the passwords with the Head Teacher/ Deputy Head.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will not open e-mail attachments unless they come from a recognised and reputable source.
9. I will bring any other attachments to the attention of the ICT technician.
10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
11. I will report immediately to the headteacher any unpleasant material or messages sent to me.
12. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
14. Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.
15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name..... Signature: .....

Date: .....

Laptop code of conduct for Dalestorth Primary and Nursery School staff

1. The laptop remains the property of Dalestorth Primary School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Dalestorth Primary and Nursery School Staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Dalestorth Primary and Nursery School.
4. When in school and not being used, the laptop must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
5.. Whenever possible, the laptop must be taken out of school and if so not be left in an unattended car. If there is a need to do so it should be locked in the boot.
6.. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
7. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
8. Any software loaded must not affect the integrity of the school network.
9. If any removable media is used then it must be checked to ensure it is free from any viruses.
10. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
11. If any fault occurs with the laptop, it should be referred to Crispin Tucker, technician.
12. The laptop would be covered by normal household insurance. If not, it should be kept in school and locked up overnight.

Name.....
Signature: .....
Date: .....

Online safety training needs – self-audit for staff

Name of staff member/volunteer:
Date:

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/carers?
Are you familiar with the filtering and monitoring systems on the school's devices and networks?
Do you understand your role and responsibilities in relation to filtering and monitoring?
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?