Bellingham Partnership of Schools

Online Safety & Mobile Phone Use Policy

Author	**Diane Grey**
Date	**January 2025**
Ratified by Governors	**February 2025**
Review date	**January 2027**

Contents:

1. Aims
2. Legislation and guidance
3. Teaching and Learning
4. Managing Filters
5. Managing emerging Technologies
6. Protecting Physical Data
7. Policy Decisions
8. Communication
9. Staff Code of Conduct – School ICT systems
10. Responsible Use Rules (pupils/students, parents/carers)

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils/students, staff and volunteers.
- 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 with and address an incident, where appropriate.
- Establish clear mechanisms to identify, intervene with and address 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 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.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design, use and monitoring.
- Safe and secure broadband from DurhamNet including the effective management of filtering and PCE forensic software for network monitoring.
- Only authorised devices are allowed connection to the school network.

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
- Filtering and Monitoring

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'/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.
This online safety policy will operate in conjunction with other policies including those for ICT, Behaviour, Bullying, Child Protection and Data Protection.

3. Teaching and learning

Why is Internet use important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
  Internet use will enhance learning
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet for research, including the skills of searching, retrieval and evaluation. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Internet access in school will include filtering appropriate to the age of pupils.
- The use of Internet derived materials by staff and by pupils must comply with copyright law.

3.1 Managing Internet Access

3.1.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be employed as part of an online safety Service Level Agreement with NCC.

3.1.2 Pupil access

- Pupil access to the Internet will only be available under supervision when all computers are visible to staff.
- All computers require a user to log in with their unique username and password, so activity can always be traced back to an individual.
- All pupils in school will receive teaching on Internet usage appropriate to their skill level and subject to the school receiving the necessary consents of both pupils and parents in agreement with the Responsible Use Rules (RUR).
- The responsible use rules will be posted in the main computer areas to allow pupils to refresh themselves with their commitment to using the Internet safely. The continued use of and access to the Internet will be subject to pupils continuing to abide by the RUR.
- Pupils will be encouraged to be critical users of the Internet, being prompted to question the truth and authenticity of information they access and to evaluate the information they retrieve.
- Downloading material from the Internet will only be undertaken with permission of the teacher responsible for that particular session. Similarly, material will not be uploaded onto the schools ICT equipment from external media devices originating outside school without permission.
- All electronic communication will be conducted within a set of guidelines taught as part of the ICT curriculum regarding the appropriate use of electronic media.

3.1.3 E-mail

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission from a parent or carer.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

3.2 Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number as well as contact information for the Governing Body.
- Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.3. Use of Images

- Many school activities involve the taking and use of images. These may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement.
- However, this interest also brings dangers. The publication of pupils' images, especially where they are accompanied by the individual's full name, could attract the wrong sort of interest.
- The school will consider carefully how these activities are organised and undertaken. Particular regard will be given when they involve young or vulnerable pupils who may be unable to question why or how the activities are taking place.

3.3.1 School Websites

- Particular care will be taken by teachers, parents and pupils when considering the publication of material onto the internet. Articles will be screened very carefully to ensure that pupils cannot be individually identified by full name or by any other means. This includes ensuring that they cannot be identified from the file name of any electronic image files that are placed on a website. Ideally, shots should be distant/groups, rather than of individual students.
- Parents who are considering setting up a private/family website with details relating to a particular school in their community, should first seek permission from the head teacher if they intend using images of other children or young people from the school or a specific setting.
- All relevant permissions will be sought prior to publication.

3.3.2 Consent

- Photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. Therefore, the use of

such images by schools requires the consent of the individual concerned as well as their parent/carer.

- The school must get parental consent before any photographs or videos of a pupil are taken where these are likely to be used in a publication or displayed by the school in a public place. (The definition of 'public place' includes areas where visitors to the school would have access to the images).
- Use of images of children requires the consent of the parent / carer. Permission will always be obtained by using the relevant form. The standard form will be used when a child joins the school roll, (or becomes a member of a related provision). This covers both the establishment and Northumberland County Council when using the photographs in publications and on websites.
- When a parent does not agree to their child being photographed, the head teacher will inform staff and make every effort to comply sensitively. For example, if a child whose parents have refused permission for photography is involved with a sports event, e.g. a football match, it may not be appropriate to photograph the whole team. Careful liaison with parents is therefore essential. With discussion it may be possible to agree on other options. The parent may accept a team photograph if names are not published or they may be prepared to consent if it affects the whole team.
- When photographic images are transmitted or shared beyond the establishment e.g. television broadcasts, or film making, specific permission will be obtained.

3.3.3 Inter-School Events including sports fixtures

- These guidelines will be applied to inter-school events. If a vulnerable student is involved, it will be necessary to liaise with a member of staff from the other establishment so that they are aware of the wishes of the parents or carer of the child, and as far as practicable to seek the cooperation of the parents of the opposing team.
- Sports facilities which are available for public usage often have strict policies restricting the use of video, mobile and still cameras. It is important therefore to check with the facility concerned as there may also be a registration process to comply with.

3.3.4 Teacher Training and Portfolios of evidence

- During teacher training and with newly qualified staff, colleagues may be required to compile portfolios with photographs of children during lessons. Staff should act responsibly in compiling these images. A member of the management team may wish to oversee the compiled images as part of the management process and consider their appropriateness.

3.3.5 Children Photographing Each Other

- This practice can occur extensively particularly during offsite activities or residential activities. There may be incidents where children take inappropriate photographs, perhaps showing friends and other students inappropriately dressed. Staff should endeavour to discourage this practice, but ultimately parents are responsible for monitoring their child / young person's use of cameras and subsequent use of their images involved.

3.4 Mobile Phones

- The use of mobile phones and the technology within the device (e.g. digital camera) is not allowed in school. Mobile telephones are to be left with the Office and collected at the end of the day. Any concerns of misuse of the mobile telephone must be reported to a senior member of staff. All mobile phones are handed into staff during morning registration and are given out at the end of the day.
- All children wearing SMART watches must ensure that their mobile phone is turned off and handed into the Office.

3.5 General Consent

- General consent will be obtained when children join the school. This general consent can be withdrawn at any time. Each year as part of a standard communication, parents will be reminded that they can change their permission.

3.6 Event Specific Consent

- It is not always possible to predict events and projects in advance. Sometimes we may want to use a photograph of a student or group and find that we don't have consent. In these cases we will have to contact parents/carers and get consent on a case-by-case basis.
- For every instance when photographs are to be used or taken by the press and media we will seek consent. This is because their circulation and coverage may

be local, national or sometimes international and the associated storylines may be so varied as to make them unpredictable

3.7 Diversity issues

- Even though we may have the consent of the parent/carer we will exercise caution and common sense when using photographs as there may be valid religious or moral grounds for objecting to a particular activity.

3.8 Safer images checklist – we will;

- Always ensure that students are dressed appropriately
- Ensure we store images securely and that they are accessed and/or used only by those with authority to do so (photographs can be stored electronically but this must be within a secure area)
- Not amend or manipulate images. (Exceptions may be where a badge has been removed or 'brushed' to protect identity or where an image needs to be 'cropped' to fit)
- Pupils' full names will not be used anywhere on the website in association with an individual photograph; photographs and other media will be selected carefully to ensure that individuals cannot be identified by name.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and the School Office will hold a list of pupils who must not have photographs uploaded onto the school website.

3.9 Social networking and personal publishing

- The school will not allow access to social networking sites.
- Pupils will be advised never to give out personal information of any kind which may identify them or their location.
- Pupils will be advised not to place personal photos and information on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

3.10 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 Chabot's such as ChatGPT and Google Bard. Bellingham Partnership of

Schools recognises that AI has many uses to help pupils learn, but may also have 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

- Bellingham Partnership of Schools will treat any use of AI to bully pupils in line with our behaviour policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed.

4 Managing filtering

- The school will work in partnership with NCC, DFE and the Internet Service Provider (DurhamNet) to ensure systems to protect pupils are reviewed and improved.
- If pupils discover an unsuitable site, it must be reported immediately to an adult who will then report the event to the online safety Coordinator. If staff discover an unsuitable site, it must be reported to the online safety coordinator. All online safety incidents will be investigated by a member of senior staff in accordance with the online safety incident flow chart provided by the Northumberland Safeguarding Children's Board.
- Senior staff will ensure that regular checks are made aided by the use of PCE forensic software to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A LightSpeed Rocket proxy server records all internet access against an individual's unique username. When the proxy is unable to identify a user automatically (for example where the internet is being accessed from a tablet which does not require a user to log on), the user is challenged to provide their username and password before any internet access is allowed.

5. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

6. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- If there is a need to transfer personal data by means of a mobile device e.g. USB data stick, the device must use encryption technology to ensure the data is protected in transit.

7. Policy Decisions

7.1. Authorising Internet access

- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- The School Office will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Pupils must agree to comply with the Responsible Use Rules.
- Parents and pupils will be asked to sign and return a consent form.

7.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

7.3 Handling online safety complaints

- Minor breaches of the RUR will be dealt with by the teacher as part of normal class discipline, following school procedures.
- More serious or repeated transgressions will be referred to a senior member of staff and may result in removal of Internet or computer access for a fixed period. Parents/carers will be informed in this event.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with by the Headteacher in accordance with the online safety incident flowchart provided by the

Northumberland Safeguarding Children's Board and the Northumberland school child protection procedures.

8. **Communication**

8.1 Introducing the online safety policy to pupils

- The Responsible Use Rules will be posted on all computers during the network login procedure and will also be displayed in the classrooms.
- Pupils will be informed that network and Internet use will be monitored and users will be reminded of this monitoring each time they logon to the school computer network. They will be required to agree with the RUR at each login otherwise network access will not be allowed.
- Online Safety forms part of the Computing curriculum and the school delivers a comprehensive online Safety scheme of work across the school.

8.2 Staff and the online safety policy

- All staff will be given the School online safety Policy and its importance explained.
- All staff will be given online safety training to ensure they remain up-to-date with current issues.
- Staff should be aware that all network activity is monitored.
- Professional conduct is essential in line with the Acceptable Use Policy for staff.

8.3 Parents and the online safety policy

- Parents' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school website.
- All pupils and parents are required to sign and return a consent form acknowledging the school's Responsible Use Rules.

9. School ICT Systems – Staff Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's online safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my use of school information systems will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my use of information systems and the internet to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to any unauthorised person.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright.
- I will report any incidents of concern regarding children's safety to the school online safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Staff Code of Conduct.

Name:…… (signature)……

10. **Responsible Use Rules**

The computers and Internet access are provided to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will be responsible for my own behaviour when using ICT and going on the Internet, just as I am elsewhere in school.
- I will only use the computers for school work and homework.
- I will only access the system with my own log-in and password, which I will keep secret.
- I will not access other people's files.
- I will only use the Internet with supervision.
- I will not intentionally seek out unsuitable material or type inappropriate onto a computer.
- If I encounter unsuitable material accidentally I will report it immediately to a teacher or other adult in school.
- I will not download material from the Internet without permission.
- I will not print material without permission and will preview my work first.
- When sending e-mail, I will not give anyone my personal information or arrange to meet anyone.
- I will only e-mail people my teacher has approved and the messages I send will be polite and sensible.
- I will not upload any files from home onto the school network without permission from a teacher
- I understand that the school may check my computer files and monitors my use of the ICT network and the Internet sites I visit.
- I understand that if I do not keep to these rules I may not be able to continue using the Internet.

Internet Access Permission Form (excerpt from school registration form completed by all parents / carers and children)

Internet access permission - Parent/Carers agreement

As the parent or legal guardian of ..... I have read and understood the school rules for responsible internet use and give permission for my child to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that pupils will be held responsible for their own actions and will be expected to abide by the Responsible Use Rules. I also understand the sanctions that may be invoked should these rules not be followed. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet.

Signature: Date:

Internet access permission - Pupils agreement

I have read and understand the school Responsible Use Rules for the internet. I will use the computer system and internet in a responsible way and obey these rules at all times.

Signature: Date: