Downholland Haksayne C.E. Primary School

Online Safety Policy

Approved by: David Chapman and Wendy Kelly

Date: 28th November 2024

Review date: December 2025

Vision for Online Safety

At Downholland Haskayne C.E. School, we aim to provide a diverse, balanced and relevant approach to ICT where security measures are balanced appropriately with effective learning and with the intention of ensuring that all children and staff are safe when using online resources. We embed our learning by following the Christian values.

Legislation

Technology and communications are rapidly changing and becoming more sophisticated. With this change comes new ways of being unsafe and feeling threatened. Online Safety (formally e-safety) has become a very important issue that is essential to address in school throughout different areas of the curriculum, to ensure that all children and adults remain safe and in control when using technology. This could range from using computers or having access to the internet or through mobile telephones. This policy applies to all members of Downholland Haskayne School's community (including staff, pupils, volunteers, parents, carers, visitors, community users etc.), who have access to and are users of the school's ICT systems. This policy seeks to ensure that the internet is used appropriately for learning which also safeguards to protect learners from harm. All staff and volunteers understand that children can be harmed online in an abundance of ways, and so follow this policy in order to best protect and educate.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Child-on-Child Abuse

Downholland Haskayne School will refer to specific guidance in Keeping Children Safe in Education Part five: Child on Child Sexual Violence and Sexual Harassment and Lancashire Procedures. 5.31 Peer Abuse (proceduresonline.com). All staff will be aware that child-on-child abuse can occur between pupils of any age and gender, both inside and outside of school, as well as online. All staff will be aware of the indicators of child-on-child abuse, how to identify it, and how to respond to reports. All staff will speak to the DSL if they have any concerns about child-on-child abuse.

All staff will understand the importance of challenge inappropriate behaviour between peers, and will not tolerate abuse as "banter" or "part of growing up".

Child-on-child abuse can be manifested in many different ways.

All staff will be clear as to the school's policy and procedures regarding child-on-child abuse and the role they have to play in preventing it and responding where they believe a child may be at risk from it.

The school will deal with such incidents within this policy (and associated behaviour and anti-bullying policies) and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place in and out of school.

Development/Monitoring/Reviewing of this Policy

This Online Safety Policy has been developed by a working group made up of:

- Headteacher
- Staff – including teachers, support staff, technical staff

Schedule for developing/monitoring/reviewing this policy: Annually

This Online Safety Policy was approved by the Governing Body on: 28th November 2024

The implementation of this Online Safety Policy will be monitored by the:

Computing Subject Leader

Headteacher

Monitoring will take place at regular intervals: Every half-term

The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

The next anticipated review date will be:

Autumn 2025

Should serious online safety incidents take place, the following external persons/agencies should be

informed:

- LA Safeguarding Officer
- LADO
- Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering

Listening to the feedback/opinions of:

- Pupils
- Parent/carers
- Staff

Key Personnel

Mr David Swindells - Headteacher, DSL

Miss Lucy Grant – Deputy DSL

Roles and Responsibilities

The Headteacher

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, although the day to day responsibility for e-safety will be delegated to all teaching staff. The Headteacher (Designated Safeguarding Lead) is aware of the procedures to be followed in

the event of a serious e-safety allegation being made against a member of staff. The Headteacher is responsible for ensuring that all teaching staff receive suitable and regular training to enable them to carry out their e-safety roles and to train other colleagues. The Head teacher will receive regular monitoring updates from the teaching staff. The Headteacher is trained in e-safety issues and will be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/stranger's potential or actual incidents of grooming
- cyber-bullying

They will:

- Keep a file of signed Acceptable Use Agreements
- Ensure that the policy is implemented and that compliance with the policy is actively monitored
- Ensure all staff are aware of reporting procedures and requirements should an e-safety incident occur
- Keep up-to-date with online safety issues and guidance through liaison with the Local Authority School's ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP)
- Provide or arrange online safety advice/training for staff, parents/carers and governors where needed (completed termly during staff meetings)
- Liaise closely with the school's Designated Senior Person to ensure a coordinated approach across relevant safeguarding areas

Network Manager/Technical Staff

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Online Safety Coordinator for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and Support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy

- They report any suspected misuse or problem to the Headteacher/ for investigation, action or sanction
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and Acceptable Use Agreement
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils

The pupils of Downholland Haskayne School:

- Are responsible for using the school digital technology systems in accordance with the Pupil Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so will be expected to know and understand the pupil policy
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice with the appropriate use of:

- Digital and video images taken at school events
- Their children's personal devices in the school (where this is permitted)

Education

Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the Pupil staying safe online policy and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need – being made to the Computing Subject Leader and Technical Staff. Only selected website pre-visited and checked by the staff should be unblocked at any one time.

It is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The four main areas of Online Safety risk are:

- Content: Pupils need to be taught that not all content is appropriate or from a reliable source
- Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies
- Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.
- Commercialism: Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications.

Children need to be made aware of the necessity to keep their personal information private, learn how to block both pop-ups and spam emails, turn off in-app purchasing on devices where possible and use a family email address when filling in online forms.

Parents/Carers

Some parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters
- Monthly targeted Online Safety newsletter
- Designated Online Safety section on the school website
- Parents evenings
- High profile events/campaigns e.g. Safer Internet Day

The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools

Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff (including students on a teaching placement) should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and staff code of conduct
- It is expected that some staff will identify online safety as a training need within the performance management process
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions
- Headteacher will provide advice/guidance/training to individuals as required

The Use of Technologies and Devices

Children

- Children are forbidden from having mobile phones on their person whilst on school premises
- Mobile games consoles are not permitted under any circumstances
- Online bullying by pupils, via texts and emails, will be treated as seriously as any other type of bullying and will be managed through our Anti-bullying / Behaviour Policy
- DfE advice; Searching, Screening and Confiscation is followed where there is a need to search a pupil for a mobile device

Staff

- Staff are permitted to have their mobile phone on their person – in a pocket or bag but they must be switched off during the school day (with the exception of staffroom and office areas) within school hours
- Staff must not access their mobile phone when children are present at any time
- No images, video or audio of children is to be recorded on personal mobile phones
- Staff may access the school's Wi-Fi on their mobile phone but for work purposes only
- On the occasion of school visits and trips off the school premises, staff may be required to take their mobile phones for emergencies
- All content and applications are purchased to comply with copyright legislation
- Content may only be transferred to school equipment and may not be transferred to personal devices/laptops

Use of Digital Media (cameras and recording devices)

Written permission for pupil's use of and access to digital media is sought from parents when the pupil joins the school and lasts for the duration of their school life. Staff are to be informed by the Headteacher whose photographs may not be taken. All images and videos of children are to be saved on the school office computer and periodically erased from school equipment. It is requested that parents who video or photograph school events, do not post this content on social media. Only school

equipment is used by staff and pupils for all school photography and film. Photographs of children will not be taken and stored on staff's own portable storage devices. Staff should remain vigilant regarding visitors' use of mobile devices

Social Networks

No social network or instant messaging sites are to be accessed in school by pupils. No social network or instant messaging sites are to be accessed by staff during teaching time and/or using school equipment. All staff need to be aware of the following points:

- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted
- If a Social Network site is used by a staff member, details must not be shared with pupils and parents, and privacy settings must be set at maximum
- Pupils must not be added as 'friends' on any Social Network site
- It is not acceptable for staff to accept, friend or follow students who are currently enrolled at the school unless they are family members
- Communication with past pupils, parents or siblings of pupils (not enrolled at school) is strongly discouraged particularly if the pupils are under the age of 18 years of age
- Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Any content posted online should not:

- Bring the school into disrepute
- Lead to valid parental complaints
- Be deemed derogatory towards school and/or its employees
- Be deemed derogatory towards pupils and/or parents or carers

Parents:

- Parents should be aware that posting inappropriate comments about individual members of staff or children can be construed as online bullying. If this situation arises then the parents(s) in question will be invited into school to discuss their issues and asked to remove the offending post
- It is not acceptable for parents to discuss issues that they may be experiencing at school on social media as it may bring the school into disrepute. We ask that the parent in question make an appointment with the relevant staff member so that their issue can be dealt with directly and then the offending post deleted
- Parents are aware that uploading images/video of their child alongside other children to social network sites is not acceptable unless specific permission has been obtained from the parents of the other children
- In the case of incidents on social media (outside of school hours) affecting children's behaviour or causing issues during school hours then a meeting will be arranged with the Headteacher and the Governor responsible, the child who has committed the incident and the child's parents to deal with the "spill over" into school hours

Email

The following statements reflect safe practice in the use of email:

- All users have access to Office Outlook Web Access through the Lancashire Grid for Learning service as the preferred school e-mail system

- Only official email addresses should be used to contact staff/pupils
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security
- All users are aware that all email communications may be monitored at any time
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature

YouTube

Children will not be able to access YouTube on classroom mobile devices or laptops. Teachers may access YouTube for teaching purposes but must thoroughly review content that they are going to use with the children before presentation to the class. YouTube may be used within the Nurture Hub under full adult supervision for sensory breaks only.

Preventing Extremism

The school is aware that it has a role to play to prevent radicalisation and extremism.

To prevent the radicalisation of young people the school:

- Has a filtering system to block out inappropriate websites
- Will report any incidents that occur
- Has received training on awareness and prevention of extremism
- Has Acceptable User Agreements in place for staff, children and anyone who may need to access the school's computers (Governors)
- Is teaching Fundamental British Values as part of the school curriculum
- Through Online Safety, teaches the children to become critical learners and so they know what is acceptable or unacceptable even though filters are in place

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a Data Protection Policy

- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- There are clear and understood policies and routines for the deletion and disposal of data and there is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- The use of cloud storage (Google Photos) meets the requirements laid down by the Information Commissioner's Office

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Infrastructure and Technology

Our school's internet is provided by Benchmark who provide internet filtering services. Sophos Anti-Virus package is provided by Lancashire.

All servers, wireless systems and cabling are securely located and access is restricted.

- Critical updates and software installation involving executable files is completed by the school technician who visits monthly
- Security breaches will be reported to the Headteacher

Pupil/Staff Access

Pupils access school equipment under the direction of the class teacher or support staff, who will be directed by the class teacher. All staff have an individual secure username and password and pupils log on with an individual username and password.

School Website

Parental consent is sought and all staff are to be aware of those pupils who do not have permission to appear on the school website (through photographs or names). Pupils should not be identifiable in pictures with captions although newsletters may contain names (excluding surnames) of children who have achieved something such as star of the week.

Dealing with Incidents

Below is an overview of how staff are required to deal with online safety incidents. All

online safety incidents must be reported to the Headteacher for logging

and further guidance where necessary. Any recorded incidents will be included in the

Headteachers Report and be reviewed by Governors.

Incident: Procedure and Sanctions:

Accidental access to inappropriate materials

- Inform a trusted adult.
- Minimise the webpage, turn the Monitor off by closing the screen on a laptop or pressing the lock button on a mobile device.
- Staff to report to Benchmark
- Persistent 'accidental' offenders may need further disciplinary action.

Using other people's logins and passwords maliciously; deliberate searching for inappropriate; materials; Bringing inappropriate electronic files from home; Using chats and forums in an inappropriate way

- Inform Headteacher
- Record incident
- Additional awareness raising of online safety issues and the AUA with individual child/class.
- More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
- Consider parent/carer involvement.

Any suspected illegal material or activity, including incidents of terrorist or extremist activity or sexting (see child protection policy), must be brought to the immediate attention of the Headteacher (DSL) who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

This policy will be reviewed annually to ensure conformance with current guidelines and in

consultation with key stakeholders.

Review due: December 2025