Darwen St James'
C of E Primary Academy

Working Together

Online Safety Policy

Mission

Nurturing ambition through living faith.

Vision

Our Academy delivers a purposeful curriculum through its living Christian faith. We nurture ambition in all our learners in order for them to become positive citizens of tomorrow.

Bible

'Let us not love with words or speech alone but with actions and truth.'

John 3:18

Document Purpose

This policy reflects the ethos of Darwen St James CE Primary Academy in relation to Online Safety. It is consistent with the Academy's agreed aims and objectives and sets out a framework within which teaching and support staff can operate.

Audience

This document is intended to give a clear outline of the Academy's approach about Online Safety to all staff, governors and parents. It is also intended for the use of the Academy's Advisory Service when assisting the development of the curriculum and for any authorised inspector. Copies of this document are provided for all teaching staff and are available when necessary to support staff and members of the Academy's Governing Body. A copy of this document is available for the use of parents.

Using New Learning Technologies Effectively and Safely

At Darwen St James, we are committed to ensuring that children learn how to use computers and modern technologies safely so that they:

- Are able to use technology safely to support their learning
- Know how to use a range of ICT equipment safely
- Are able to use modern technologies outside Darwen St James in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology and ICT

Enhancing Learning through using the Internet

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Writing and Reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for Computing, Computing Security, Anti Bullying and for Child Protection. Miss Peckson, Miss Lawson and Ms Earp are the Child Protection Coordinators. The Computing Coordinator is the Online Safety Coordinator. The Online Safety Policy was revised by the Online Safety Coordinator.

Leadership of Online Safety

Leadership of Online Safety Our Online Safety lead is our Computing Curriculum Lead. The responsibilities of the online safety lead alongside the Online Safety group are to:

- Ensure membership of the Online Safety group represents a range of stakeholders in the school community
- Maintain own knowledge of wider Online Safety and online safety leadership through training, seeking advice, and signing up to regular updates
- Carry out an Online Safety audit to inform the review process
- Regularly review the effectiveness of Online Safety policy and practice
- Ensure the computing curriculum is progressive and age appropriate and that there opportunities across the wider curriculum including PSHE to reinforce Online Safety messages.
- Ensure all Academy staff receive Online Safety training annually and that a record of training is maintained
- Provide updates on Online Safety policy and practice to governors
- With the Academy's technical support, ensure that appropriate filtering and anti-virus software is in place
- Maintain reporting procedures for Online Safety incidents - This may be part of a wider reporting system, but should include access to inappropriate resources (intentional or otherwise), inappropriate use of Academy technology, Online Safety and cyberbullying disclosures. There should also be a record of how it was dealt with and any consequences e.g. additional online safety input; discussion with parents restricting access etc.
- Provide or source Online Safety information and training for parents Ensure that appropriate acceptable use agreements are signed by pupils and parents and that permission for use of images and video is sought from parents (and pupils when appropriate)
- Ensure that the educational potential and possible online safety issues are investigated before using new technology.
- Annually review the Academy's Online Safety strategy, policy and practice

Online Safety Education and Training

The Internet is an essential element in 21st century life for education, business and social interaction. Darwen St James has a duty to provide students with quality Internet access as part of their learning experience. Current guidance stipulates that it is not sufficient to keep pupils safe in school. It is our responsibility therefore, to ensure they have opportunities to learn how to stay safe and deal with the risks associated with the internet and communication technology in the world around them. Keeping our children safe involves educating all members of our Academy's community, including governors, parents and all staff working at Darwen St James.

Our Online Safety Curriculum

At Darwen St James we ensure that children have access to a progressive Online Safety curriculum across all year groups.

Early Years Foundation Stage - Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.

In order to safely select and use technology we believe that children in the Foundation Stage need to be taught an age appropriate Online Safety curriculum. When working towards this Early Learning Goal we will ensure our children use technology safely so that by the time they leave the Foundation Stage they are ready to access the key stage 1 curriculum.

The National Curriculum 2014 for Computing stipulates that pupils:

In **key stage 1** are 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.

In **key stage 2** are taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

In **key stage 3** 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.

In **key stage 4** understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to identify and report a range of concerns.

At Darwen St James we use a number of approaches to ensure our pupils are confident and safe users of technology in and out of school. To ensure pupils have access to an age-appropriate Online Safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote Online Safety through teaching pupils how to stay safe, how to protect themselves from harm, we:

- Introduce age appropriate school and classroom rules each year and reinforce them regularly
- Use progressive statements within Purple Mash, to ensure that areas of online safety relating to communication, information, creating and presenting ideas, and Computer Science are covered regularly. These are planned into computing, PSHE and where possible the creative curriculum.
- Deliver online safety messages in assembly in response to need, to reinforce national initiatives and agendas such as Safer Internet Day and anti-bullying week.
- Before using a new device or online resource, pupils are taught how to use it safely and appropriately. This is reinforced regularly.
- Teach pupils to tell a trusted adult should they be worried or upset by anything they encounter online or using communication technology. (All staff are made aware of what to do if a pupil confides in them.)
- The need to keep login details and other personal information private will be reinforced regularly when using the schools network, learning platform and any other methods of communication agreed by the Headteacher.

Pupils will be taught how to evaluate Internet content appropriate to their age.

Darwen St James will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught what Internet use is responsible and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age group.
- Pupils will be taught about the dangers of radicalisation and extremism at an appropriate level for their age.

Responsibility for Internet Content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to Dataspire through Every, and if required, to the DSL via My Concern.
- It is a shared School responsibility to ensure that the use of Internet derived materials by staff and by pupils comply with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Risk Assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the

school nor BwD can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head Teacher and ICT Co-ordinator will ensure that the Internet policy is implemented and compliance with the policy monitored.

Filtering and Monitoring of Internet Content

- The Academy will work in partnership with parents, the LEA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider.
- The Network Manager will ensure that every possible effort is made to filter offensive or dangerous content.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that we believe is illegal must be referred to the Internet Watch Foundation.
- Filtering strategies will be selected by the Academy, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.
- Any attempt by staff or pupils to purposely access inappropriate material will be referred to Senior Management and dealt with in accordance with Academy policy.

Educating Parents/Carers

Children often seem more at home in the digital world than their parents. To ensure that children are the safest they possibly can be, we must educate parents about the risk of using the internet and communication technology for their children and the potential for their own use of technology to place themselves or their child at risk. We ensure parents receive information and training by:

- Providing links to information and resources for parents on our Academy website, Class Dojo and Facebook page.
- Inviting parents to join Online Safety sessions or attend Online Safety assemblies.
- Encouraging parents to act as role models when using technology.

The school will share with parents and children, our belief that:

- The unsupervised use of social network spaces intended for adults outside school is inappropriate for pupils of primary age.
- PEGI and BBFC ratings are good indicators of how appropriate the levels of violence, sexual content, bad language and the portrayal of drug taking and criminal acts are.
- Family friendly filtering can help to keep children safe, however education and the opportunity to develop safe practice is essential for keeping children safe.

- Pupils who use the internet and other communication technology may be at risk of being groomed or radicalised. It is important that parents understand that secrecy is a possible factor in both of these.
- What pupils do online now, can affect their future life. If a child is happy to tell a parent or carer when they are worried, they are the safest they can possibly be; therefore we encourage parents to nurture a sense of trust between them and their child when talking about using technology.

There are some excellent online tools for reporting concerns, such as the Report Abuse button which can be found on the https://www.thinkuknow.co.uk/ site and Childline: http://www.childline.org.uk . Children are also encouraged to report their concerns via a member of staff or trusted adult.

Educating Staff and the Wider Academy Community

- We ensure that all new staff receive online safety training and all Academy staff have access to basic online safety training regularly, through the BwD Me Learning Platform and Purple Mash.
- The online safety lead and key members of the online safety group have access to a higher level of training, updates and information to ensure that they have the skills and knowledge necessary to lead all areas of Online Safety.

Basic training includes

- Online Safety issues for pupils
- Reporting procedures
- Guidance on appropriate use of communication technology by staff and pupils
- Guidance for staff on how to stay safe
- Expectations in terms of passwords and data security
- Expectations in terms of professional conduct including the use of social media
- Teaching pupils to minimise the screen if they see something that makes them feel uncomfortable.
- Online Safety training references and complements guidance in the Safer Working Practices document.

Keeping Staff and Pupils Safe at Darwen St James

All access to the internet is filtered. Darwen St James will work with Cidari, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the online safety Lead who will inform the Cidari E Learning Manager so that they can take appropriate action.

All users will be taught how to care for devices in terms of health and safety. This includes avoiding placing food or liquids near to electrical devices, carrying equipment and rules around charging and electrical sockets. The Academy internet access is designed expressly for pupil use and includes appropriate filtering. Sanctions for inappropriate use of the internet and communication technology will be explained to the children. A record of any misuse is kept by the Head teacher. At Darwen St James and the staff do not use their

own personal devices/accounts to contact parents and pupils. To protect staff and pupils, Darwen St James provides a phone for contacting parents when on trips and visits and Academy email addresses. Cameras and ipads/Fire's are provided for recording Academy related activities. Images of children should not be taken or stored on personal devices.

Darwen St James uses social networking such as Facebook to communicate with parents, here is an outline of our practice.

- Anyone can post on the school Facebook page however posts are approved by the administrators.
- A select number of staff have editing rights and responsibilities.
- The Academy refrains from tagging anyone as it is a general information page to inform parents and carers of events, celebrations and important information linked with the Academy.
- If faced with unwanted communication the administrators are advised to block content.
- There is no group or group membership set up on the page.
- Parental permission is sought in order to upload images and information about children and Academy activities.
- In order to maintain privacy for the staff, they have all agreed to not communicate with the Academy's Facebook page.
- Staff must not communicate with parents or children through their own social media accounts

Passwords security

- Pupils are encouraged to keep their password private.
- Parents are encouraged to ask children to logon to their accounts and show them what they have been doing rather than ask children to share their passwords.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils may only use approved digital methods of communication on the school system. E.g. communication tools through the school website/Purple Mash
- Pupils in key stage 2 upwards will be taught about the report abuse button (this can be found on many websites including our school website) through the Online Safety lessons.
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Webcams will only be used with staff supervision.

Reporting Online Safety Concerns

Children are encouraged to report their concerns via a member of staff. We also encourage the children to use national resources such as Hector and CEOP.

Detail below systems for reporting online safety concerns. This should build on any systems for behaviour and safeguarding already in school. It should include:

- Online safety concerns to be reported on My Concern. The nature of the incident and action taken are recorded with any consequences e.g. additional online safety input; discussion with parents restricting access etc.. This includes access to inappropriate resources (intentional or otherwise), inappropriate use of Academy technology, online safety and cyberbullying disclosures.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Complaint procedures regarding the Internet at Darwen St James

• Responsibility for handling incidents will be delegated to a senior member of staff.
• Any complaint about staff misuse must be referred to the Head Teacher.
• Pupils and parents will be informed of the complaints procedure.
• Parents and pupils will need to work in partnership with staff to resolve issues.
• As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
• Sanctions available include:
- interview/counselling by Head Teacher;
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including home learning.

Published Content

Any information that can be accessed outside the Academy's intranet should be classed as published whether in electronic or paper format.

- Electronic communication 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.
- General contact details should be the Academy address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. (This may be through education and guidance, as directly reading everything is impractical)
- Where pupils publish work, there will be systems in place to check the content and pupils will be given clear guidelines about what can be published.

Publishing Pupils Images and Work

Staff and pupils using digital cameras, video recorders, Ipads or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner. (In the Foundation Stage this may not be practical when capturing a child in the process of learning, however should be modelled as often as possible.) Photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs or video of pupils are published. Where pupil's work is published Darwen St James will ensure that the child's identity is protected. Where Academy events are being publicised, care will be taken not to reveal information that may put children or staff at risk e.g. the date and location of a trip.

The Management of Email

- 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 details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to external personal email accounts may be blocked if it is felt that their use is of no educational benefit.
- Excessive social email use can interfere with teaching and learning and may be restricted.
- All pupils on roll and all staff will be given a school Google email account, this supports the use of Google Classroom.
- Email 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.
- The forwarding of offensive material is strictly prohibited.
- Teachers should always remember that an email sent from the school email system carries the school's name, and as such should be treated as official.
- Teachers should take professional responsibility for ensuring that external correspondence has been verified through the expected channels.
- The Head Teacher has the authority to request a check of emails without written permission, if they feel that the online safety policy is not being applied.

Parents Using Still or Video Cameras

In line with the Information Commissioner's Office, Darwen St James does not allow parents to record video and images during performances. We advise parents of this before each event.

Authorising Internet access

All staff must read and sign the 'Responsible ICT Use Agreement' before using any Academy ICT resource. The Academy will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. Parents will be asked to sign and return a consent form for their children to access the internet.

Assessing risks

Darwen St James will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer. Neither Darwen St James nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the e safety coordinator and to the LA where necessary. The Academy will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

Handling online safety complaints

Complaints of Internet misuse will be dealt with by the Headteacher and where appropriate inform the LA. Any complaint about staff misuse must be referred to the Headteacher OR Chair of Governors Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures. Pupils and parents will be informed of the complaints procedure on request.

Communications Policy

Introducing the online safety policy to pupils

- Online safety will be the first unit taught in each year group.
- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

Introducing the policy to parents

Parents' attention will be drawn to the Academy Online Safety Policy and practice:

- On Class Dojo
- On the Academy website
- On social media
- Internet Safety Week

Staff and the Online Safety policy

All staff will be given the AcademyOnline Safety Policy and its importance explained. Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential. The Academy may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on Academy equipment.

Management of the School Website

- The point of contact on the Web site should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless permission is received.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.

- The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the Academy's guidelines for publications.
- The copyright of all material must be held by the Academy, or be attributed to the owner where permission to reproduce has been obtained.

Staff Responsibility

- All staff must accept the terms of the online safety statement before using any Internet resource in school.
- Staff will need to show their ability to monitor student safety, by accepting the terms of the online safety statement.
- By accepting a network account, all members of staff are agreeing to abide by and promote the responsible use of the Internet.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff which operate monitoring procedures will do so under the supervision of senior management and will only do so on signing a confidentiality contract.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

School ICT system maintenance and Security

- The Academy ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LEA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Pupils' files held on the Academy's network will be regularly checked.
- The ICT Co-ordinator will ensure that the system has the capacity to take increased traffic caused by Internet use.

Review/Evaluation of This Policy

The policy will be reviewed by the Computing coordinator on an annual basis in consultation with the Headteacher, staff and the Link Governor. Acceptable Use Policy, ICT scheme and assessment procedures will be reviewed and adapted to keep pace with curriculum developments and developments within ICT technology.

Policy reviewed - October 2020