DARWEN VALE
An Aldridge Community Academy

E-Safety Policy

Policy Title:	E-Safety Policy
Version:	1.0
Approval Date:	1/7/2021
Date Of Next Review:	30/6/2022
Policy Upholder:	David Smalley

School E-Safety Policy

Contents

Statement of Purpose

Darwen Vale High School and Engineering College are committed to using new learning technologies effectively and safely to enable a positive contribution to be made to pupil experiences allowing higher expectations to be achieved.

Our E-safety Policy has been written taking into account DFE guidance, Keeping Children Safe in Education to ensure pupils, school employees and parents are capable of taking full advantage of access to information in a safe environment.

The purpose of this E-safety policy is to:

- Safeguard and protect all of the Darwen Vale community online.
- Identify approaches to educate and raise awareness of online safety throughout the school community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Scope

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for safeguarding.

- Mr A Bradley is the schools E-safety Co-ordinator who will work in collaboration with the DSL Mr D Smalley

- The E-Safety Policy and its implementation will be reviewed annually, in response to an incident, or following any new government legislation or guidelines.

Teaching and Learning

Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. However, it is vital children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that they are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which Darwen Vale are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Why Internet use is important

New technologies have become integral to the lives of children and young people in society. The internet and other digital and information technologies are powerful tools, which open up new learning opportunities for everyone.

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.

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

- The school will ensure that the use of Internet derived materials by school employees 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.
- Sanctions for inappropriate use of the internet will be explained to the children.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Use of Technology in school

- Pupils may only use the internet when supervised by a school employee
- All school devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- All files stored on the school computers will be treated as school property
- Our ICT Service Provider and Smoothwall technology will keep a check of sites visited by users and key words or phrases which could be a cause for concern
- Internet use is for school related work only, not personal use
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home
- Personal information about any user should not be revealed on the internet
- Staff will use age appropriate search tools following an informed risk assessment or change request, to identify which tool best suits the needs of our students.
- School will ensure that the use of internet-derived materials, by staff and learners complies with current copyright and data protection laws and acknowledge the source of information.
- Sending, displaying, accessing, creating (or trying to do these) any obscene or offensive material is not permitted
- Downloading games, executable programmes and unlicensed software is not permitted
- The use of the Internet for financial gain is not permitted
- Only e-mail addresses provided by the school should be used by pupils and staff
- Access to ‘chat rooms’ is not allowed
- Any misuse of the internet should be reported immediately to a member of staff
- The school will have the right to withdraw access to individuals

Managing Internet Access

Information system security

- We will maintain a record of users who are granted access to our devices and systems.
- All staff, pupils and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.
- School ICT systems capacity and security will be reviewed regularly.
- Firewalls and virus protection is updated regularly.

Managing filtering

We have based our filtering and monitoring settings based on guidance from our filtering and monitoring technology partners and UK safer Internet Centre documentation on establishing 'appropriate levels' of filtering and monitoring: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Staying safe

The school will ensure that pupils and parents are aware of E-safety issues. A list of useful addresses and resources is included in this document. Pupils may only use approved digital methods of communication on the school system e.g. not forwarding chain letters.

- Darwen Vale will appropriately monitor internet use on all organisational devices provided access to our internet services. This is achieved by:
    - Physical monitoring (supervision)
    - Monitoring internet and web access (reviewing logfile information)
    - Live technology monitoring services through our filtering, logs and firewalls.
    - Daily/Weekly alert review of positives and false positives alerts via Smoothwall technology.
    - Monthly report reviews and analysis of trends and behaviours.

- If a concern is identified via monitoring approaches:
    - DSL and staff members will respond in line with the child protection and safeguarding policies and procedures.
    - Raise a Change Request when appropriate to block or allow certain URLs or filtering categories. Any member of staff can submit a Change Request with the school IT helpdesk by email or phone. This request will be reviewed by the IT Cluster Manager, DSL and Director of IT as appropriate considering the nature and urgency of the issue. Any safeguarding concerns will be dealt with immediately.

- All users are informed that all use of Darwen Vale systems and services are monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- Curriculum time is used for staff to explain how the internet should be used safely.

- 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 and school employees 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.
- Monitoring and filtering measures does also include guest access
- All Darwen Vale devices have monitoring software installed. Devices will be monitored at all times independent of the location or internet provider. This software monitoring all internet activity in the devices regardless of the user.
- For Chromebooks, the monitoring is based on user, regardless of Chromebook used (organisational owned or personal). For the rest of the devices, monitoring is based on device, so personal devices are not affected.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in our school are bound. Through our E-Safety Policy, we will ensure that we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

The school might impose disciplinary penalties for inappropriate behaviour which include incidents of cyber-bullying, or other Online Safety incidents covered by this policy, as well as the behaviour and safeguarding policies, which may take place outside of the school, but are linked to pupils and staff of the school, or where there is evidence that the behaviour could be deemed as bringing the school into disrepute

As a school we make sure that our students and staff have the knowledge, tools, processes and training necessary to deal with any E-safety incidents in a restricted or unrestricted Internet environment. Promoting a safe use of internet technologies in a ubiquitous way.

Published content

Any information that can be accessed outside the school'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 school address, e-mail and telephone number. Employee or pupils' personal information will not be published.

The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

- Photographs and/or videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or videos of pupils are published.
- Where pupil's work is published the school will ensure that the child's identity is protected.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

Policy Decisions

Authorising Internet access

- All school employees must read and sign the 'Responsible ICT Use Agreement' before using any school ICT resource. **Please see Appendix 1**
- The school will keep a record of all employees 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. **Please see Appendix 2**
- Pupils have a child friendly version for the guidelines in their school planners, this page must be read, signed and understood before use is allowed.

Responsibilities

- All users must show a high degree of responsibility when using the internet
- School employees have a responsibility to monitor access whilst pupils use the internet
- The Head of Faculty or nominated appropriate person will investigate any cases of misuse by pupils and, in conjunction with the e-Safety Co-ordinator, decide if individuals should have access withdrawn
- The school will ensure the correct level of monitoring access is achieved
- The Local Governing Committee (LGC) will monitor that guidelines are being followed
- Parents have a responsibility to monitor the home environment and encourage pupils to always use the internet in a safe manner

Security

Darwen Vale takes appropriate steps to ensure the security of our IT systems, including:

- Virus protection being updated regularly.
- Encryption for all personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files, permissions and sharing settings held on our network and organisational cloud managed environments.
- The appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended and appropriate timeouts have been setup.
- Further information about technical environment safety and security can be found at the IT Security Policy.
- All users will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- We require all users to use strong passwords for access into our system and some will require 2 factors of authentication for security reasons.
- We will post appropriate information about safeguarding, including online safety, on our school websites for members of the community. The E-safety officer on each school will audit and update each year the information provided in line with the Trust E-safety yearly programme.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and where appropriate inform the LA.
- Any complaint about employee misuse must be referred to The Principal.

- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaint's procedure on request.

Roles and Responsibilities

Principals:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy *and/or* acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

Designated Safeguarding Leads (DSL):

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside senior leaders and pastoral teams to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.

- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns in line with Aldridge Education Trust child protection and safeguarding policies and procedures.

Staff members:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site. Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area

Pupils:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

Parents and carers:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the E-Safety and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Review

The E-Safety Policy and its implementation will be reviewed annually, in response to an incident or following any new government legislation or guidelines.

Appendix 1

Darwen Vale High School and Engineering College
Responsible ICT Use Agreement

The use of e-technology equipment owned by Darwen Vale for personal use is really a question of circumstance i.e. in-school or at home. Each circumstance must be considered on its merits.

Insurance is the responsibility of the individual when used off premises and the equipment must be returned in clean, good working order.

The use of school equipment and facilities can be a motivational factor to some employees and could easily be seen as a means to self-INSET i.e. using a piece of equipment for a personal reason would improve familiarity and confidence with the equipment thus leading to improved learning in the school.

Any equipment that is borrowed must be through the SBMs Office, for a specified length of time, no 'long-term' loans will be permitted.

Computers

Many employees have laptop computers that must predominantly be used for school related work. In the past it has been accepted that some personal use would be allowed from home e.g. the downloading of images to burn onto a CD. Under current tax laws if the computer is used in any way for personal matters it must be declared as a pecuniary interest. The simple upshot is that a school laptop should not be used for personal interests otherwise it should be declared on a tax form.

Cameras and Video

The school has several pieces of equipment that are available for school employees to use.

Mobile Phones

The use of the school mobile phones is outlined in a separate document (See School Handbook), but it should be noted that the use of private mobile phones is strictly prohibited in the classroom and they should only be used away from pupils in personal time.

Software

The usual licensing agreement for software is that it should not be placed on any computer that is not owned by the school. Although several enlightened companies do allow education professionals to use their software at home for educational use, preparing lessons etc. (Promethean being one) It is important that each agreement is checked before any installation is carried out. All software licensing queries should be directed to the Internet Service Provider at Darwen Vale.

Software approval packages should be installed by the Service Desk on to computers. After the approval time they should be removed if not required or purchased through the normal channels.

Email

Most school employees are provided with an e-mail address from out ICT Service Provider in the form of anamexxx@darwenvale.learningfutures.org.uk (a name relates to the person, xxx is a 3-digit random number). This should predominantly be used for professional use e.g. circulars from BwD etc.

Any communication with pupils or parents must be via this email account, under no circumstances should a private email account be used. Any communication with parents should use this server address. All these emails should be kept in a separate folder called 'Parents'. It is acknowledged however that you may use this address for a certain amount of personal email, provided that this does not impinge on school time or the smooth running of the school. Other personal email accounts e.g. hotmail should not be accessed from school.

Internet

Access to the Internet from school for personal use should be strictly limited to times outside the normal working day and then be carefully considered. (Never in a classroom situation) It should be remembered that the school and Local Authority have monitoring software that logs all Internet use. School 'firewalls' should never be disabled and the downloading of executable files is prohibited due to risk of attack by computer viruses. If you wish to download programs in special circumstances, the school Service Desk must be consulted before the download.

Personal social networking sites should never be accessed from school and no school data or pupil information should ever be displayed or discussed. Academic forums are a useful source of information for educators but please be aware of the context, who are the people on these forums?

Note on Data Protection

It is a criminal offence to attempt to corrupt or maliciously attack data stored in a bona-fide manner i.e. all data on the school system.

It is also the responsibility of all users to safeguard that data. Personal information such as SEN data, class registers, personal information etc. should never be displayed in a manner that would allow other people to see that data. Beware of leaving the computer screen turned on, they should always be 'locked' by the user if the screen is left for any length of time. Similarly you should avoid the physical transport of such data on memory devices as these are easily misplaced or lost. If data is lost please inform the the network manager immediately.

Your school login is personal to you and should not be given out to any other person.

Your data is of utmost importance to you. You must always ensure your own data is backed up securely, in order that your data can be restored in the case of catastrophic failure. Any data saved on any school network drive is automatically backed up by the school system each evening. Note the C: drive on your machine is not automatically backed up.

School Monitoring of Information

The school has a system that monitors each and every web page, email, word document etc. for offensive and unacceptable content. The school reserves the right to use this system to monitor all information passed via the school network.

Pupil safety

Every time school employees use the school system the safety of the children must be the paramount. Should employees discover any possible incidents of a safeguarding nature, they must inform the school E-Safety Coordinator or the Safeguarding Coordinator immediately.

Signed _____

Dated _____

Appendix 2

DARWEN VALE HIGH SCHOOL
ENGINEERING COLLEGE and EXTENDED SCHOOL

INTERNET USER AGREEMENT

I, the undersigned pupil, request access to the Internet and agree to abide by the following rules and regulations:

1 Access to the World Wide Web (hereafter known as the Web) is exclusively for the purposes of furthering and supporting my education.

2 I will not attempt to access any material or information on the Internet which might be considered to be inappropriate. This is taken to mean any site that carries information, of whatever format that is of a pornographic, violent, racist, sexist nature, which promotes any illegal activity, or in any other way is deemed to be inappropriate by the Head teacher.

3 I agree to access only those sites that are providing information which supports my education. This is taken to exclude the use of the Internet for personal investigations, unless permission has been approved by the member of staff in charge and that site or sites being visited have been viewed and approved by that member of staff.

4 I understand that access to the Web is only allowed between the hours of 8am and 6pm on normal school days in school. If a school portable device is used to access the web at any time, all other rules and regulations still apply. I am aware that this access is also monitored and therefore is not private.

5 I accept that an email account will be provided; the account will have an address of the form anamexxx@darwenvale.learningfutures.org.uk

6 I agree that all my use of the school network will be monitored and therefore is not private.

7 I understand that offensive language is prohibited within emails. Use of offensive language or otherwise inappropriate messages will result in the suspension or removal of my account from the network. Further disciplinary action may be taken by the school and may result in temporary exclusion.

8 I am responsible for ensuring that my password remains confidential and, as such, if another person accesses my account and breaches any of the regulations, I will be held responsible. If I believe that my password is known by someone else, I must report it to a member of staff.

9 If any of these rules are broken, my Internet access will be removed and my access to the system suspended or removed permanently. For school portable devices this may result in it being taken back by the school.

Name of pupil: Form:

Pupil's signature:

I, the parent or carer of the above pupil, have read the above and wish my son/daughter to have access to the Internet to support their education. I understand that if they break the agreement, they will be disciplined and that, in certain circumstances, this may result in temporary exclusion from the school.

Signature of parent/carer: Date:

Appendix 3

DARWEN VALE HIGH SCHOOL & Blackburn with Darwen Local Authority

MOBILE LEARNING PROJECT EXTENSION AGREEMENT

This document is an agreement between the Local Authority, school, users and parents, and shall be binding for the length of the scheme.

Blackburn with Darwen LA will:

- routinely evaluate the success of the project and report findings to relevant authorities.

School will:

- provide training in the use of the ultra mobile computers for learners.
- ensure that quality learning opportunities are provided for learners to develop their use of the devices.
- routinely assess the progress of the learners.
- provide wireless internet provision for learners to access web based materials at any time from within school.
- monitor the use and effectiveness of ultra mobile devices as an enhancement to learning.

Learners will:

- use their ultra mobile devices responsibly to improve their ICT skills and learning in other subjects.
- report any faults or problems to the school.
- follow the safety rules within our E safety Policy
- use their ultra mobile computer both at home and at school and encourage their parents to work with them on joint activities.
- take great care with their ultra mobile device, ensuring that it is charged and in school each day.
- give opinions about what works successfully and what needs to be improved.

Parents will:

- support their child's use of the ultra mobile device and share work and projects with them.
- support the school to ensure that safe and responsible internet practices are followed.
- report any faults or issues to the school.
- find opportunities to develop their own ICT skills alongside their child.
- support involvement, with their children, in the evaluation and publicity of the project.

I …….. agree to the terms and conditions above.

Signed…… (Learner)

Signed …… (Parent)

Signed…… (Darwen Vale High School)

Appendix 4

Ultra Mobile Learning

Blackburn with Darwen LA Mobile Learning Project Extension

Digital Photography/Digital Video Parent or Guardian Consent form

As part of our Ultra Mobile Learning Project we intend to use digital photography, digital video and audio recording to record key events for the purpose of evaluating the project. This will be motivating for the pupils involved and provide an excellent opportunity to publicise and promote this cutting edge 21st century learning.

Please read and complete the following.

I consent to digital images, sound files and video of the child named below to be taken where appropriate and printed in any project publications, used in local and national presentations and posted on the Blackburn with Darwen Learning Platform and school website.

I acknowledge that the images may also be used in and distributed by other media, such as CD-ROM and as part of general promotional activities surrounding the aims of the school and local authority.

I understand that still images, audio and video will be used only within the outlines of the project as explained to me in the agreement form and that the identity of my child will be protected.

Name of School _____

Name of Child _____

Name of Parent or Guardian _____

Address _____

_____

Signature _____

Date _____

Please direct any queries regarding this form to the headteacher of your child's school. Thank you for your continued support in this exciting project.
Please return to your child's school