REACH
LEARNING PROVISION

IT AND E-SAFETY POLICY

Date Produced: August 2022

Review Date: September 2023

Next Review Date: September 2024

Introduction

The E-Safety Policy (Education) has been created to ensure that children and young people are able to use the internet and related communication technologies as part of the wider duty of care to which all who work in education are bound. In addition, this policy enables staff to identify and manage risks, safeguard and support staff, student, and parents/Carers by promoting the safe use of technology.

Keeping Children Safe in Education (2022) outlines the responsibility that schools and the Designated Safeguarding Lead (DSL) have in ensuring that all students, young people, and staff use electronic technologies in a safe and productive way. Technology is advancing quickly and can be sued in a beneficial and positive way to educate and develop the young people we work with. However, measures must be taken, and procedures and processes followed to ensure the safeguarding of all young people who use this technology. In addition, technology and social media play an important part in the social development and learning of young people, it is the DSL's responsibility to ensure leaders, managers and staff are fully aware of statutory updates and requirements to ensure the safeguarding of young people. The DSL is also responsible for the delivery of information. Advice and Guidance for young people and parents/carers so that they are informed and empowered to use technology and social media in a safe way, and that they know that they can disclose concerns, particularly surrounding grooming, CSE sexting, sexting, the sharing of illicit images and online bullying, in a safe and confident way. This policy is intended to be used in conjunction with the REACH Learning Provision Safeguarding Children and young People Policy.

What is the policy about?

The purpose of this Online Safety Policy is to:

- Clearly identify the key principles expected of all members of REACH Learning Provision education community with regards to the safe and responsible use of technology to ensure that the provision is a safe and secure environment.
- Safeguard and protect all members of the REACH Learning Provision education community online.
- Raise awareness with all members of the REACH LEARNING PROVISION education community regarding potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

Who is the policy for?

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for or provide services on behalf of REACH (collectively referred to as 'staff' in this policy) as well as young people and parents/carers.

Policy statement and requirements

Making use of ICT and the Internet in the Provision

The Internet is used in the provision to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the provision's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education, and business. We want to equip our students with all necessary ICT skills that they will need to enable them to progress confidently in their educational careers and onward towards their working environments when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For Students

- unlimited access to worldwide educational resources and institutions such as art galleries, museums, and libraries
- contact with schools in other countries resulting in cultural exchanges between students all over the world
- access to subject experts, role models, inspirational people, and organisations. The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet
- an enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally
- self-evaluation; feedback and assessment; updates on current affairs as they happen
- access to learning whenever and wherever convenient
- freedom to be creative
- freedom to explore the world and its cultures from within a classroom
- social inclusion, in class and online
- access to case studies, videos, and interactive media to enhance understanding
- individualised access to learning.

For staff

- professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies
- immediate professional and personal support through networks and associations
- improved access to technical support
- ability to provide immediate feedback to students and parents
- class management, attendance records, assessment, and assignment tracking.

For parents

- Communication between the school and parents/carers may be through the provision e-mail and telephone messages. This form of contact can often be more effective, reliable, and economic. Text messages and letters will also inform parent/carers of details relating to attendance, behaviour, and other appropriate matters.

The Role of Teaching and Support Staff

- have an up-to-date awareness of E-Safety matters from the DSL and the current E-Safety policy and practices
- have read, understood, and signed the Staff Acceptable Use Agreement (AUA)
- report any suspected misuse or problem to the Provision Manager and E–Safety Coordinator (DSL) for investigation
- ensure that all digital communications with students/ parents/ carers should be on a professional level and only carried out using provision systems
- embed E-Safety in all aspects of the curriculum and other activities
- ensure students understand and follow the E-Safety and Acceptable Use Agreements
- ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other provision activities and implement current policies regarding these devices
- ensure that where internet use is pre-planned, students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches

The Role of the Designated Safeguarding Lead(s)

To receive appropriate training (through the Local Children's Safeguarding Board) on E-Safety issues and be aware of the potential serious safeguarding/ child protection issues to arise from:

- The sharing of personal data
- Access to illegal/ inappropriate materials
- Inappropriate on-line contact with adults/ strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting and the sending of inappropriate images including self-images

N.B. It is important to emphasise that these are Child Protection and Safeguarding issues, not simply technical issues i.e., the technology provides additional means for Child Protection issues to develop.

The Role of Students and Young People

- are responsible for using the provisions digital technology systems in accordance with the Student Acceptable Use Agreement
- 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, understand, and comply with policies on the use of mobile devices and digital cameras
- will be expected to know, understand, and comply with policies on the taking/ use of images, sexting and on cyber-bullying
- should understand the importance of adopting good E--Safety practice when using digital technologies out of the provision and realise that the school's E-Safety Policy covers their actions out of the provision, if related to their membership of the provision.

The Role of Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The provision will take every opportunity to help parents/carers understand these issues through home/provision liaison.

Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at the provision
- their children's personal devices at the provision

Communicating Provision Policy

This policy is available from the provision office and on the provision website for parents/carers and staff.

Rules relating to the provisions code of conduct when online and E-Safety guidelines will be displayed around the school. E-Safety is integrated into the curriculum where the internet or technology are being used and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. We will therefore seek to provide information and awareness to parents and carers through curriculum activities and high-profile events and campaigns e.g., E-Safety Day.

Training

Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- annual e-safety training from the DSL.
- all new staff will receive E-Safety training as part of their induction ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements
- the E-Safety Co-ordinator(s) (DSL(s)) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this E-Safety Policy and its updates will be presented to and discussed by staff, as appropriate in meetings
- the E-Safety Co-ordinator(s) (DSL(s)) will provide advice/ guidance/ training to individuals, as required

4. Learning to evaluate Internet Content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent.

This is approached by the provision as part of digital literacy across the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the provision will take any intentional acts of plagiary very seriously; for students who are found to have plagiarised, appropriate action will be taken.

The provision will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites, then the URL will be reported to the school E-Safety Co-ordinator (DSL). Any material found by members of the provision community that is believed to be unlawful will be reported in accordance with policies and procedures. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

Managing Information Systems

REACH Learning Provision is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of provision data and personal protection of our provision very seriously. This means protecting the provision network, as far as is practicably possible, against viruses, hackers, and other external security threats.

The security of the provision information systems and users will be reviewed regularly, and virus protection software will be updated regularly.

Some safeguards that the provision takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted/ password protected
- ensuring that unapproved software is not downloaded to any provision computers.
- files held on the provision network will be regularly checked for viruses
- the use of user logins and passwords to access the provision network will be enforced portable media containing provision data or programmes will not be taken off-site without specific permission from a member of the senior leadership team
- Regular reporting to the Provision Manager
- For more information on data protection in school, please refer to the REACH Learning Provision GDPR and DATA Policy

E-mail

REACH Learning Provision uses email internally for staff and externally, for contacting parents. It is an essential part of provision communication. It is also used to enhance the curriculum. It may also be used to provide immediate feedback on work and requests for support where it is needed. Staff and students should be aware that provision email accounts should only be used for provision-related matters, i.e., for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The provision has the right to monitor emails and their content but will only do so if it feels there is reason to.

Provision Email Accounts and Appropriate Use

Staff should be aware of the following when using email in provision:

- staff should only use official provision-provided email accounts to communicate with students, parents, or carers; personal email accounts should not be used to contact any of these people for provision business

- emails sent from provision accounts should be professionally and carefully written; staff represent the provision whilst at work and should take this into account when entering any communication
- staff must tell their manager or a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the provision or from an external account; they should not attempt to deal with this themselves
- the forwarding of chain messages is not permitted in provision

Students should be aware of the following when using email in provision:

- REACH does not issue student email accounts.
- they will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the provision network or their personal wellbeing.

Using photographs of individual students

REACH Learning Provision website is viewed as a useful tool for communicating our ethos and practice to the wider community. It is also a valuable resource for parents/carers and students by providing information. The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the provision, copyrights, and privacy policies. No personal information on staff or students will be published, and details for contacting the provision will be for the provision office only

REACH follows these general rules on the use of photographs of individual students:

- Parental consent must be obtained for external/promotional use- see above.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that photographs are appropriate for the public domain.
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group
- Parents/ carers are not permitted to take photographs or videos whilst on the provision premises.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or events, they are being asked to participate in.

Any official photographers that are commissioned by the provision will be fully briefed on Child Protection matters in relation to their work, will always wear identification, and will not have unsupervised access to students at any time.

Complaints of misuse of photographs or video Parents/ carers should follow the standard REACH Learning Provision complaints procedure if they have a concern or complaint regarding the misuse of school photographs. You can find our complaints procedure on our website or speak to a member of staff who will be able to direct you through the process.

Social networking, social media, and personal publishing

REACH Learning Provision follows the following rules on the use of social media and social networking sites at the provision:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the provisions' code of conduct regarding the use of ICT and technologies and behaviour online including sexting. This is delivered through PSHE lessons.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Students and staff are not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful, or defamatory. The provision expects all staff and students to remember that they are always representing the provision and must act appropriately.
- Safe and professional behaviour of staff online will be discussed during the staff induction process.

Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly.

Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues, including the sharing of inappropriate or illicit images and sexting.

REACH Learning Provision adopts a zero-tolerance policy in relation to electronic devices owned by students and brought onto provision premises in relation to the making and distribution of images and/ or recordings of students and staff.

We do; however, understand that a parent/carer may wish for their child to have a mobile phone for their journey to and from the provision. In this situation a student should adhere to the following procedure:

Emergencies:

- If a student needs to contact his parents/carers, a school phone will be made available.
- If parents/carers need to contact their child urgently they should phone the provision office and a message will be relayed promptly.

Responsibility:

- REACH accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices including those handed in.
- REACH will not investigate the theft, loss or damage relating to student phones/devices.

Staff:

- Under no circumstances should staff use their own personal devices to contact students or parents either in or out of provision time unless in an emergency.
- Staff are not permitted to take photos or videos of students on personal devices. If photos or videos are being taken as part of a provision activity or for a professional capacity, the provision's equipment will be used for this.
- REACH expects staff will lead by example: Personal mobile phones will be switched off or placed on 'silent' and stored away in a safe location during teaching hours.
- Any breach of provisions policy may result in disciplinary action being taken against that member of staff.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the provision. If an allegation of bullying does come up, the provision will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine provision systems and logs or contact the service provider to identify the perpetrator.
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the perpetrator that this behaviour will not be tolerated. Appropriate action will be taken, as necessary.

Managing Emerging Technologies

Technology is progressing rapidly, and new technologies are emerging all the time. REACH will risk-assess any new technologies before they are allowed in the provision and will consider any educational benefits that they might have. The provision keeps up to date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting Personal Data

REACH believe that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-provision and individual progress. The provision collects personal data from students, parents, and staff and processes it to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision. We take responsibility for ensuring that any data that we collect, and process is used correctly and only as is necessary, for full and comprehensive information on how the school safeguards data, refer to the REACH's Data Protection policy.

Unsuitable/ inappropriate activities

Any of the following activities are deemed inappropriate in school:

- the accessing of pornography
- the promotion of any kind of discrimination
- the use of threatening behaviour, including promotion of physical violence or mental harm
- using any other information which may be offensive to colleagues or breaches the integrity of the ethos of the provision or brings the provision into disrepute
- using provision systems to run a private business
- using systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the provision
- infringing copyright
- revealing or publicising confidential or proprietary information e.g., financial, personal information, data bases, computer / network access codes and passwords
- creating or propagating computer viruses or other harmful files
- unfair usage
- on-line gaming, educational and non-educational
- on-line gambling
- the use of social media without permission
- the use of messaging apps without permission
- the use of videoing broadcasting or YouTube without permission

Responding to Incidents of Misuse

Illegal incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there are any other suspected illegal activity REACH reporting procedures should be followed as outlined in the REACH Safeguarding Children and Young People policy.

Other incidents

It is hoped that all members of the provision will be responsible users of digital technologies, who understand and follow REACH's policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- More than one senior member of staff should be involved in the process and the incident reported following the REACH Safeguarding Children and Young People Policy. This is vital to protect individuals if accusations are subsequently reported.
- The procedure should be conducted using a designated computer that will not be used by students and if necessary, can be taken off site by the police should the need arise. The same computer should be used for the duration of the process.
- Relevant staff should have appropriate internet access to conduct the procedure, and sites and content visited closely monitored and recorded to provide further protection.
- The ULR of any site containing the alleged misuse and the nature of the content causing concern should be recorded. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. This may be printed, signed, and attached to the form (except in cases of child sexual abuse).
- Once fully investigated the group should judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following: -Internal response or discipline procedures -Involvement by Local Authority or national/ local organisations (as appropriate) -Police involvement and/ or action If content being reviewed includes images of child abuse, then the matter should be referred to the Police immediately.

Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child and from child to child.
- the inclusion of adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or material isolate the computer in question as best you can. Any changes to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and the police and demonstrate that visits to these sites were carried out for child protection purposes.

School Actions and Sanctions

It is more likely that the provision will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in an appropriate manner, and that members of the provision community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal REACH behaviour/ disciplinary procedures and could include:

Students

- Referral to class teacher / tutor
- Referral to E-Safety Co-ordinator(s)
- Referral to Line Manager
- Referral to Headteacher
- Referral to the Police
- Referral to Technical Support staff for action re filtering/ security etc.
- Informing parents / carers
- Removal of network / internet access rights
- Revised Risk Assessment
- Issue of a Warning
- Detention or sanction
- Fixed Term Exclusion
- Permanent Exclusion

Staff

- Referral to Line Manager
- Referral to Headteacher
- Referral to Local Authority/ HR
- Referral to Line Manager
- Referral to Technical Support staff for action re filtering etc.
- Enhanced Risk Assessment
- Warning
- Referral to agency/ counselling
- Suspension from duty
- Disciplinary action
- Referral to the Police
- Dismissal

Related policies

This policy must be read in conjunction with Keeping Children Safe in Education (2022) and other relevant school policies including (but not limited to) REACH Safeguarding of Children and Young People Policy, Anti-bullying Policy, Behaviour Policy and PSHE Policy.