Brigantia Learning Trust
Online Safeguarding Policy

Version	1.0
Author including Title	Adam Kubica – Network Manager
Responsible committee	Finance, Risk and Audit
Date adopted	08/11/2019
Review Date	09/11/2020
Target Audience	All stakeholders
Related Documents	Data Protection Policy
Referenced	

Contents

Introduction

The Brigantia Learning Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. The use of technology is encouraged in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that the Trust is also aware of potential risks and challenges associated with such use. The Trust approach is to implement safeguards across the Trust and to support staff, children and young people to identify and manage risks independently. This can be achieved through a combination of security measures, training and guidance, and the implementation of our policies. In furtherance of our duty to safeguard staff and learners, the Trust will aim to ensure that staff and children/young people stay safe online.

Online safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology, and provides safeguards and awareness for users to enable them to control their online experiences. The online world is developing rapidly and most of our children/young people have access to devices which enable them to connect to the internet, take images, videos and communicate with others. The use of these exciting and innovative tools in our academies and at home has been shown to raise educational standards, and promote the achievement of children/young people. However, the use of these new technologies can put users at risk. As stated previously, the breadth of issues within online safeguarding is considerable, but they can be categorised into three areas of risk:

Content: being exposed to illegal, inappropriate or harmful material
Contact: being subjected to harmful online interaction with other users
Conduct: personal online behaviour that increases the likelihood of or causes harm

Many of these risks reflect situations in the offline world so it is essential that this Online Safeguarding Policy is used in conjunction with other policies including the Trust Safeguarding and Child Protection policies.

This policy applies to all members of the Trust community including staff, children/young people, Directors and visitors who have access to the Trust IT systems, both on the premises and remotely. Any user of Trust IT systems must adhere to the current age-appropriate Acceptable Use Agreement.

Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

Roles and Responsibilities

Online Safeguarding is the responsibility of each academy and everyone in them has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for teaching and learning. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Principal/Headteachers:

The Principal/Headteachers have overall responsibility for online safeguarding all members of the academy, though the day-to-day responsibility will be delegated to the Trust Online Safeguarding Team and the Safeguarding Leads in each academy.

Responsibilities of the Trust Online Safeguarding Team:

The team will ensure that the Trust's Online Safeguarding Policy and Acceptable Use Agreements are current, appropriate and reviewed regularly. The team will promote the safe use of the internet and any technologies used within the academies to the staff and children/young people.

The team includes the Safeguarding Leads, ICT staff, technical staff and staff with responsibility for Personal and Social Education from each academy in the Trust and is chaired by the Trust Inclusion Lead.

Responsibilities of the Teaching and Support Staff:

Online communication should normally be done through the Trust hosted systems, e.g. Trust email and Virtual Learning Environments. All staff must keep personal and professional lives separate online and maintain a professional level of conduct in personal use of technology at all times. All staff are responsible for using the Trust IT systems and mobile devices in accordance with the Acceptable Use Agreements, which they must actively promote through the Tutorial/PSE programme, subject lessons and general good practice. They must also take steps to ensure their own safety online. Staff are responsible for modelling safe behaviours to the children/young people at all times.

All staff are responsible for ensuring the safety of learners and appropriate use of the internet and IT systems. They must report any concerns immediately. Where this relates to educational misconduct, concerns should be reported to their line manager. Where this relates to a potential safeguarding issue, concerns should be reported to a member of the Safeguarding Team.

Responsibilities of the Safeguarding Lead in Each Academy:

The Safeguarding Lead in each academy is responsible for ensuring that appropriate training about online safeguarding is delivered to staff, promote online safety within the academy and to parents/carers, and oversee any online safeguarding incidents, supported by technical staff.

Responsibilities of Technical Staff:

Technical staff will support the Trust by providing a safe, technical infrastructure to support teaching and learning. They will ensure that access to the network is only through an authorised, restricted mechanism and that provision exists for misuse detection and against malicious attack. They will ensure that access controls exist to protect personal and sensitive information held on school-owned devices. They will report any online safeguarding issues to the appropriate Safeguarding Team.

Responsibilities of Children/Young People:

Children/young people are responsible for using the Trust IT systems and mobile devices in accordance with the age-appropriate Acceptable Use Agreement. Children/young people will attend online safety lessons as part of the tutorial, PSE lessons, ICT lessons or assemblies. They should respect the feelings, rights, values and intellectual property of others in their use of technology both in and beyond the academy. They are expected to seek help and follow procedures where they have concerns, where they believe an online safety incident has taken place involving them or another member of the community. They must act safely and responsibly at all times when using the internet or other mobile technologies.

Responsibilities of Parents/Carers:

Parents/carers should help and support the Trust by promoting online safeguarding including the Acceptable Use Agreement with their children/young people. They should consult with the academy if they have any concerns about their children/young people's use of technology.

Responsibilities of the Directors:

They will monitor and support the work of the Trust`s Online Safeguarding Team in promoting and ensuring safe and responsible use of technology in any Trust-related activities including appointing named Safeguarding Governors, and encouraging parents/carers to become engaged in online safeguarding activities. They will ensure appropriate funding and resources are available for the Trust to implement its online safeguarding strategy.

Education and Training

With the current unlimited nature of internet access, it is impossible for the academies to eliminate all risks for staff and learners. The Trust must support staff and learners through training and education which will provide them with the skills to be able to identify risks independently and manage them effectively.

Learners:

Children/young people will learn about online safety as part of their Tutorial/PSE and ICT programmes, through assemblies and the computing curriculum. They will be reminded about their responsibilities through an age-appropriate Acceptable Use Agreement which they must agree and adhere to. Children/young people will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. They will receive information about potential dangers associated with online safety, e.g. sexting, social media use and image sharing, and legal implications. Within classes, they will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect copyright and to cite references properly.

Managing ICT Systems and Access

The Trust has a responsibility to ensure that all elements of its infrastructure and ICT services are as safe and secure as possible. All staff and children/young people`s access to Trust-owned equipment and ICT services is controlled through the use of age- appropriate username and password complexity policies. It is important that all children/ young people and staff have an awareness of how to construct a complex and secure password as well as understanding the security implications of not protecting the password once selected.

Access to systems is always based on a least -privilege approach and only after being approved by a Headteacher/Principal or Director.
Every effort is made to keep security software up to date. Appropriate security measures include the use of enhanced filtering and protection of firewalls, servers, routers, workstations, etc. to prevent accidental or malicious access of Trust systems and information.

Internet Filtering and Firewalls:

Each academy's internet filtering is set to an appropriate level based on the user accessing the internet. Any amendments made to the filtering are assessed by the Trust's technical team and/or SLT prior to implementation.

With authority from the Principal/Headteachers, internet filtering and firewalls are regularly tested by the technical team for effectiveness and feedback passed to the Trust provider.

Antivirus Protection:

All academies within the Trust have antivirus protection across all the end user devices and servers set to an appropriate level of protection to protect the network infrastructure from virus threats.

Remote Access:

The Trust has a number of systems available as online services to encourage teaching and learning beyond the classroom in the form of VLE's, intranets, email, remote desktop and virtual private networks (VPN's).

The Trust utilises Cloud Computing services provided by third party providers for many aspects of data storage such as storage of user and Trust data, email and data backups to increase data availability from multiple devices The Trust ensures that all Cloud Computing providers used are on the DFE's approved providers' list for education and conform to the Data Protection Act and the Trust's Data Protection Policy.

Staff and children/young people primarily use services already provided by the Trust. However, prior to staff and children/young people utilising additional Cloud services, they should enquire with the technical team and data controller to ensure that the provider conforms to the above.

Use of Personal Devices (Bring Your Own Devices - BYOD):

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by users bringing their own technologies in order to provide a greater freedom of choice and usability. However, the Trust recognise that there are a number of online safety considerations for BYOD that need to be regularly reviewed. Use of BYOD should not introduce vulnerabilities into existing secure environments.

Devices should only connect to the advertised BYOD wireless network to ensure a robust filtered internet connection and protect the Trust's network infrastructure. Users are responsible for the condition of the device brought to an academy, including updates, antivirus software and repair.

Children/young people may only make use of BYOD when given permission by a member of staff or at agreed times of the working day and abide by the academy behaviour policy. If a child/young person breaches academy policy, then the phone or device may be confiscated and held in a secure place in the academy. Mobile phones and devices will be released to parents or carers in accordance with the academy policy.

Data Protection

For further information, refer to the Brigantia Learning Trust Data Protection Policy.

Responding to Incidents of Misuse

The Trust will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Agreements.

All members of the Trust community must be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or deliberate misuse. Any incidents will be dealt with as soon as possible in a proportionate manner through the academies` behaviour/disciplinary procedures. Where conduct is found to be unacceptable, the academies will deal with the matter internally. Where conduct is considered illegal, the academies will report the matter to the police.

The Trust will not tolerate any abuses of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with children/young people and staff disciplinary procedures. The academy will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

If a child/young person wishes to report an incident, they can do so to any member of staff. Educational misconduct, e.g. plagiarism, will be reported to the appropriate manager; safeguarding incidents to the Safeguarding Teams. When a member of staff wishes to report an incident, they will contact their line manager or a member of the SLT.

Mobile Phone Usage in Academies

It is recommended that staff do not use their own mobile phone devices for communicating with children/young people whilst on educational visits or use the camera/video on their mobile phone in class, wherever possible.

Children/young people will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Use of Social Media

It is recommended that any contact with pupils and parents/carers only takes place via Trust approved communication channels, e.g. academy email address or the learning platform, so it can be monitored and traced in the case of an allegation or concern.

However, the Trust recognises that in some cases there may be pre-existing relationships which mean that any “ban” from adding children/young people or parents/carers as friends or contacts on personal social networking sites may be difficult to enforce. It is, therefore, recommended that members of staff are encouraged to make SLT aware of these exceptions in order to protect themselves from allegations or misinterpreted situations.

It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status. Staff are advised to check their privacy settings on any personal social media sites they use. However, they should always remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is thought to have been deleted or privately shared). Staff can obtain further advice from ICT or Technical staff in each academy.

Protecting the Professional Identity of All Staff, Work Placement Students and Volunteers

Communication between adults and between children/young people and adults, by whatever method, should be transparent, and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, emails, digital cameras, videos, web-cams, websites, forums and blogs.

Responsibilities of Staff

When using digital communications, staff should (unless there is a pre-disclosed relationship):

- Only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the academy.
- Not share any personal information with a child or young person, e.g. should not give their personal contact details to children and young people including personal email, home or mobile telephone numbers, social media identities.
- Not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child/young person under 19 years or parent/carers on social networks.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with children/young people so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the Trust into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.
- Only make any social media posts after, not during, an event.
- Not geotag locations of children/young people whilst on a trip/visit.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children/young people's instant use of images that they have recorded

themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The academies will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate children/young people about the risks associated with the taking, using, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet. e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow Trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Trust equipment. Unless permission is obtained from SLT, personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that children/young people are appropriately dressed and are not participating in activities that might bring the individuals or the Trust into disrepute.
- Children/young people must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children/young people will be selected carefully, and will comply with good practice guidance and relevant legislation on the use of such images. Images should not be used of any children in care or young people who are accommodated.
- Children/young people`s full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website or VLE.
- Children/young people's work can only be published with the permission of the child/young person and parents or carers.
- When searching for images, video or sound clips, staff should use image banks where possible and children/young people will be taught about copyright and acknowledging ownership

Appendix 1:

Response to an Online Safeguarding Incident of Concern