Buckler's Mead Academy

Policy Document

ON-LINE SAFETY POLICY

Policy Title:	Online Safety Policy
Responsible Person:	Safeguarding / Paul Mattocks
Document Reference:	SPOL/MAN1118/023
Date Produced/Reviewed:	November 2018
Recommended by (Advisory Group / Committee / SLT):	Behaviour & Safeguarding
Date Adopted:	November 2018
Date published on website (if applicable):	December 2018
Signed By:	 …… Chair of Directors
Review Frequency:	Annually
Review Term:	Autumn 2019
Please note: The version of this document contained within the 'Policy Documents' Folder on BMStaff (T:\Admin\Policies and Procedures) is the only version that is maintained.	

Buckler's Mead Academy Online Safety Policy 2018.

Contents

1. Introduction and Overview

Rationale - The purpose of this policy is to:

- Set out the key principles expected of all members of the academy community at Buckler's Mead with respect to the use of ICT-based technologies.
- Safeguard and protect the students and staff at Buckler's Mead Academy.
- Assist academy staff working with students to work safely and responsibly with the internet, other communication technologies and to monitor their own standards and practice.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other academy policies.
- Ensure that all members of the academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our academy community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games, substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content
- radicalisation

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords
- child sexual exploitation

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))

- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)

Copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope

This Online Safety policy (formally E-safety) applies to all members of the academy community (including staff, students , volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

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

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies. The academy will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of academy.

The policy draws on work produced by the Lgfl and SWgfl as well as containing input from students at Buckler's Mead Academy. It should be read in conjunction with the academy's safeguarding policy as well as the relevant sections of Keeping Children Safe in Education 2018.

Role	Key Responsibilities
Headteacher	• Overall responsibility for Online Safety provision, data and data security • Ensure the academy uses an approved, filtered Internet Service, compliant with current statutory requirements • Ensure that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant • Be aware of procedures to be followed in the event of a serious Online Safety incident. • Receive regular monitoring reports from the Online Safety Co-ordinator / Officer • Ensure that there is a system in place to monitor and support staff who carry out internal Online Safety procedures (e.g. network manager)
Online Safety Co-ordinator / Designated Child Protection Lead	• Day to day responsibility for Online Safety issues and establishing and reviewing the academy Online Safety policies / documents • Promote an awareness and commitment to e-safeguarding • Ensure that Online Safety education is embedded across the curriculum • Liaise with academy ICT technical staff • Communicate regularly with SLT and the designated Online Safety Director to discuss current issues, review incident logs and filtering / change control logs

Role	Key Responsibilities

	• Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
	• Ensure that an Online Safety incident log is kept up to date
	• Facilitate training and advice for all staff
	• Liaise with relevant agencies
	• Keep up to date with in Online Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Directors / Online Safety director (Mr R Hunt)	• Ensure that the academy follows all current Online Safety advice to keep the children and staff safe • Approve the Online Safety Policy and review the effectiveness of the policy. • Support the academy in encouraging parents and the wider community to become engaged in Online Safety activities • Appoint an Online Safety Director who will: Regularly review with the Online Safety Co-ordinator / Officer (including Online Safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• Oversee the delivery of the Online Safety element of the Computing curriculum • Liaise with the Online Safety coordinator
Technicians	• Report any Online Safety related issues to the Online Safety coordinator. • Ensure that users may only access the academy's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • Ensure that provision exists for misuse detection and malicious attack • Ensure the security of the academy ICT system • Ensure that access controls / encryption exist to protect personal and sensitive information held on academy-owned devices • Apply and update on a regular basis the academy's policy on web filtering • Keep informed of issues relating to the filtering applied by the Grid • Keep up to date with the academy's Online Safety policy and technical information • Regularly monitor use of the network / Virtual Learning Environment / email in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator /Headteacher for investigation. • Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Keep up-to-date documentation of the academy's e-security and technical procedures
Data Protection Lead	• Ensure that all data held on students on the academy office machines have appropriate access controls in place in compliance with the GDPR 2018

Role	Key Responsibilities
Teachers	• Embed Online Safety issues in all aspects of the curriculum and other academy activities • Supervise and guide students carefully when engaged in learning activities involving online technology (including extracurricular and extended academy activities if relevant) • Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• Read, understand and help promote the academy's Online Safety policy and guidance • Be aware of Online Safety issues related to the use of personal devices. Monitor their use and implement current academy policies regarding these devices • Report any suspected misuse or problem to the Online Safety coordinator • Maintain an awareness of current Online Safety issues and guidance • Model safe, responsible and professional behaviours • Ensure that any digital communications with students should be on a professional level and only through academy-based systems.
Students	• Read, understand, and adhere to the Acceptable Use Policy • Have a good understanding of research skills, the need to avoid plagiarism and uphold copyright regulations • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology. • Know and understand academy policy on the use of personal devices. • Know and understand academy policy on the taking / use of images and on cyber-bullying. • Understand the importance of adopting good Online Safety practice when using digital technologies out of academy and realise that the academy's Online Safety Policy covers their actions out of academy, if related to their membership of the academy • Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in academy and at home • Help the academy in the creation/ review of Online Safety policies
Parents/ carers	• Support the academy in promoting Online Safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the internet and the academy's use of photographic and video images • Read, understand and promote the academy Student Acceptable Use Agreement with their children • Access the academy website / LEARNING PLATFORM / on-line student / student records in accordance with the relevant academy Acceptable Use Agreement. • Consult with the academy if they have any concerns about their children's use of technology

Handling complaints:

- The academy will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of

change, it is not possible to guarantee that unsuitable material will never appear on an academy computer or mobile device. The academy cannot accept liability for material accessed, or any consequences of Internet access.

- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with academy child protection procedures.

2. Education and Curriculum

Student Online Safety curriculum

This academy

- Has a clear, progressive Online Safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student sees on before logging in to academy computers.
- Ensures staff will model safe and responsible behaviour in their own use of technology
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include buying on-line; on-line gaming / gambling.

Staff and Director training

This academy

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training available to staff on Online Safety issues and the academy's Online Safety education program.
- Provides all staff (including those on university/college placement and work experience) with information and guidance on the Safeguarding policy and procedures.

Parent awareness and training

This academy

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Suggestions for safe Internet use at home;
    - Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct
In this academy, all users:

- Are responsible for using the academy ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to read before being given access to academy systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of academy and realise that the academy's Online Safety Policy covers their actions out of academy, if related to their membership of the academy
- Will be expected to know and understand academy policies on the use of personal devices. They should also know and understand academy policies on the taking / use of images and on cyber-bullying

Staff - Are responsible for reading the academy's Online Safety policy and using the academy ICT systems accordingly including the use of personal devices.

Students

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management
In this academy:

- There is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
- Support is actively sought from other agencies as needed in dealing with Online Safety
- Parents / carers are specifically informed of Online Safety incidents involving young people for whom they are responsible.

- We reserve the right to contact the police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

- **Internet access, security and filtering**

This academy:

- Uses educational filtering systems which block sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies to define access levels.
- Ensures all staff and students understand that they must report any concerns;
- Ensures students only publish within an appropriately secure environment.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the network manager/ IT technicians.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities .

- **Network management (user access, backup)**

This academy

- Uses individual, audited log-ins for all users

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful
- Has local network auditing software installed
- Stores data within the academy and online in accordance with the GDPR 2018

To ensure the network is used safely, this academy:

- Ensures staff read and sign that they have understood the academy's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the academy's' management information system is controlled through a separate password for data security purposes;
- Provides students with an individual network log-in username.
- Ensures students have their own unique username and password which gives them access to the Internet and Google apps for Education.;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the academy, is used solely to support their professional responsibilities and that they notify the academy of any "significant personal use" as defined by HM Revenue & Customs
- Maintains equipment to ensure Health and Safety is followed.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data;

- Ensures that access to the academy's network resources from remote locations by staff is restricted and access is only through academy approved systems.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides students and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password.
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted.
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the academy ICT systems regularly regarding health and safety and security.

Passwords policy

- This academy makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access academy systems. Staff are responsible for keeping their password private.

E-mail

This academy

- Provides staff with an email account for their professional use.
- Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

Students:

- Students are introduced to and use e-mail as part of the Computing scheme of work.
- Students are taught about the safety and 'netiquette' of using e-mail both in academy and at home i.e. they are taught:
    - Not to give out their e-mail address unless it is part of an academy managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - That an e-mail is a form of publishing where the message should be clear, short and concise;
    - That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on academy headed paper;
    - They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    - To not open attachments unless sure the source is safe;
    - That they should think carefully before sending any attachments;
    - Embedding adverts is not allowed;
    - That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - Not to respond to malicious or threatening messages;
    - Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - That forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff can only use the academy e mail on the academy system
- Staff only use academy e-mail for professional purposes
- Access in academy to external personal e-mail accounts may be blocked
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on academy headed paper. That it should follow the academy 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;

Academy website

- The Headteacher takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;

- The academy web site complies with the statutory government guidelines on content;
- Most material is the academy's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the academy address, telephone number and general email contact address. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the academy website;
- We do not use embedded geodata in respect of stored images

Social networking

Academy staff will ensure that in private use:

- No reference should be made in social media to students , parents / carers.
- They do not engage in online discussion on personal matters relating to members of the academy community
- Personal opinions should not be attributed to the academy.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this academy:

- The Data Protection Lead is a member of SLT.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record

  We ensure ALL academy stakeholders understand their responsibilities with regard to data security, passwords and access.
- We follow appropriate guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the academy and limit such data removal.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- We require staff to log-out of systems when leaving their computer.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet.
- We comply with the WEEE (Waste Electrical and Electronic Equipment, European) directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the academy (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

6. Equipment and Digital Content

Personal devices

- Mobile phones and devices brought into academy are entirely at the staff member, students & parents' or visitors' own risk. The Academy accepts no responsibility for their loss, theft or damage.
- Student mobile phones may only be used in accordance with the academy's behaviour policy.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The Academy reserves the right to search the content of any student device on the academy premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the academy day, they should do so only through the Academy's telephone.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the academy site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal academy time (unless as part of an approved and directed curriculum-based activity with consent from a member of staff).
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The Academy accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety.

- If a student breaches the academy policy, then the phone or device will be confiscated and will be held in a secure place in the academy office. Mobile phones and devices will be released to parents or carers in accordance with the academy policy.
- Phones and devices must not be taken into examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use an academy phone.

Staff use of personal devices

- Any staff personal handheld devices, including mobile phones and personal cameras used for work must be noted in academy – name, make & model, serial number. Any permitted images or files taken in academy must be downloaded from the device and deleted in the academy before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families.
- Staff should not use their personal mobile phone during lessons or other paid work time.
- Personal mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose **unless** authorised by a member of SLT.
- Staff must not **keep** photographs or personal contact details of students, ex-students (under the age of 18) or parents on personal devices**.**
- If a member of staff breaches the policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for academy duties, for instance in case of emergency during off-site activities, then an academy mobile phone will be provided and used. In an emergency where a staff member doesn't have access to an academy-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this academy:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the academy agreement form
- We do not identify students in online photographic materials or include the full names of students in the credits of any published academy produced video materials / DVDs;
- The academy blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- Students are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or academy. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.