



Branston Church of England Infant Academy

Online Safety Policy

*Travelling together to be **the best we can be** within the love of God*

Policy Co-ordinator: Mrs L Cook

Original Policy Dated: March 2018

Reviewed Policy Date: March 2026

Presented to Academy Committee: March 2026

Date to be Reviewed: March 2027

Cycle Review: Annually

Policy Statement

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

Users - refers to all staff, the governors, school volunteers, pupils and any other person working in or on behalf of the school, including contractors such as Computeam.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. Parent, Guardian, Carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Term - refers to a whole term i.e. 3 whole terms a year.

Wider school community – pupils, all staff, volunteers, governors and parents.

Safeguarding is of the utmost importance in our school community. At Branston Church of England Infant Academy, we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as Online Safety or E-Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any possibility of harm to the pupils or liability to the school.

This policy is available for anybody to read on the Branston Church of England Infant Academy website. Upon review all members of staff will sign to indicate that they have read and understood the E-Safety Policy. The Pupils Acceptable Use Policy will be sent home at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Academy Committee

The Academy Committee is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any Online Safety incident, to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-Safety incidents are/were appropriately dealt with and ensure the policy is/was effective in managing those incidents.
- Ensure their own online training via Flick is up to date and monitor completion of relevant training across the school.

Headteacher

Reporting to the Academy Committee, the Headteacher has overall responsibility for E-Safety within our school. The day-to-day management of this will be delegated to a member of staff, the E-Safety Officer, as indicated below:

Mrs Lianne Cook – Headteacher & Mrs Newton – Computer Subject Lead

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team, governors and parents. ALL staff members complete annual Online Safety CPD on Flick. This also includes all members of our Academy Committee.
- The designated E-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All E-Safety incidents are dealt with promptly and appropriately and recorded in the E-Safety incident log.

E- Safety Officer

The day-to-day duty of the E- Safety Officer is devolved to Mrs Newton and in her absence the Business and Operations Partner.

The E- Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and Academy Committee on all Online Safety matters.
- Engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with the LAAT, Local Authority, IT technical support and other agencies as required.
- Retain responsibility for the Online Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the LAAT, Local Authority and/or ICT Technical Support.
- Make themselves aware through communication with Computeam of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible Local Councilor to decide on what reports may be appropriate for viewing.

Computer Technical Support Staff

We outsource our technical support to Computeam

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any Online Safety technical solutions such as Internet filtering are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety Officer and Headteacher.
 - Only allow Social Media platforms to be enabled on request of the Headteacher.
 - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters and will be changed termly.
 - Two Factor Authentication is in place.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher.

- Any Online Safety incident is reported to the E- Safety Officer and in their absence the Business and Operations Partner (and an Online Safety Incident report is made). The folder for this will be held in the School Office. If you are unsure whether the matter is to be raised, seek advice from the Online Safety Officer or the Headteacher.

All Pupils

The boundaries of use of computing equipment and services in this school are given in the Pupil Acceptable Use Policy; any deviation or misuse of computing equipment or services will be dealt with in accordance with the Behaviour and Anti-Bullying Policy.

Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. We will have a yearly training day delivered by an appropriate professional to pupils, staff and parents. Similarly, all pupils will be fully aware of how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent's evenings, school newsletters and a yearly training session the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that pupils are empowered to stay safe online.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the Pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Parents will also be made aware of why we filter the internet and our right to monitor their child's online activity and why we do this (see Appendix 1).

Technology

Branston Church of England Infant Academy uses a range of devices including laptops and Apple iPads. In order to safeguard our pupils and in order to prevent loss of personal data we employ the following assistive technology:

Monitoring and Filtering - All staff, pupils and parents of pupils will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites

Internet Filtering - we use ESET Endpoint Antivirus software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and content of the website and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher (see Appendix 1).

Email Filtering - we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message (see Appendix 1).

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; any breach (i.e. loss/theft of device such as laptop or USB key-drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the LAAT to

ascertain whether a report needs to be made to the Information Commissioner's Office (Note: Encryption does not mean password protected).

Passwords – Pupils in each class will be able to access school laptops and computers by using a class username; this will give them restricted access to the school system. All staff will have their own username and passwords assigned to them for using the laptops and school PC's and will change their passwords termly. The iPads all have a pin code which the staff know and use to unlock the iPads for the children to use.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated daily for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key-drives are not to be used without prior permission from the Headteacher.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted to pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and reiterated here for clarity. All parents must sign a photo/video release form upon joining the school; non-return of the permission form will not be assumed as acceptance.

Incidents - Any Online Safety incident is to be brought to the immediate attention of the Online Safety Officer, or in their absence the Headteacher. The Online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Branston Church of England Infant Academy will have an appropriate annual program of training.

iPad – Each iPad is numbered, and every child is allocated an iPad so that user and usage can be easily tracked.

Online Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupils learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The E-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the E-Safety Officer and then the Headteacher for further CPD.

Other Related Policies, Reports and Signposts

- Keeping Children Safe In Education (KCSIE)
https://assets.publishing.service.gov.uk/media/66d7301b9084b18b95709f75/Keeping_children_safe_in_education_2024.pdf
- RSHE Policy (compliant with the RSE Statutory Guidance September 2021)

- Review of Sexual Abuse In Schools & Colleges June 2021 [Review of sexual abuse in schools and colleges - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/news/review-of-sexual-abuse-in-schools-and-colleges-june-2021)
- www.branston-infant.lincs.sch.uk our school website which contains a separate 'Online Safety' page for both children and parents in addition to a 'Computing' page under the 'Curriculum' tab.



Acceptable ICT Use Policy – Year 1 and Year 2

Our Charter of Good Online Behaviour

All Internet and email activity is subject to monitoring

I Promise - to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise - not to look for or show other people things that may be upsetting.

I Promise - to show respect for the work that other people have done.

I will not - damage the ICT equipment if I accidentally damage something I will tell my teacher.

I will not - share passwords with anybody. If I forget the password, I will let my teacher know.

I will not - use other people's usernames or passwords.

I will not - share personal information online with anyone.

I will not - download anything from the Internet unless my teacher has asked me to.

I will - let my teacher know if anybody asks me for personal information.

I will - let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will - be respectful to everybody online; I will treat everybody in the way that I want to be treated.

I understand - that some people on the Internet are not who they say they are, and some people can be unkind. I will tell my teacher if I am ever worried in school or my parents if I am at home.

I understand - if I break these rules there will be consequences of my actions and my parents will be told.

Pupil Name: _____

Signed (Pupil): _____

Signed (Parent): _____

Date: _____



Acceptable ICT Use Policy - Foundation Stage

Our Charter of Good Online Behaviour

All Internet and email activity is subject to monitoring

I Promise - to only use the school ICT as my teacher has asked me to.

I Promise - not to look for or show other people things that make me sad.

I Promise - not to say unkind words about children's work.

I Promise - to be gentle with the school's ICT equipment, if I accidentally break something I will tell my teacher.

I will not - use other people's usernames or passwords.

I will not - tell people my name, where I go to school, or where I live when I am on the internet.

I will not - search the internet without an adult.

I will - let my teacher know if anybody asks me my name, where I go to school, or where I live.

I will - let my teacher know if anybody says or does anything to me that is unkind or upsets me.

I will - be kind to everyone when I am online.

I understand - that some people on the Internet are not who they say they are, and some people can be unkind. I will tell my teacher if I am ever worried in school or my parents if I am at home.

I understand - if I break these rules there will be consequences of my actions and my parents will be told.

Pupil Name: _____

Signed (Pupil): _____

Signed (Parent): _____

Date: _____

Appendix 1

Why we Filter and Monitor the Internet

Introduction

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the Online Safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

Very broadly speaking:

- **Filtering** - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- **Monitoring** - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

These terms are important; mention to anyone that you are monitoring their Internet use and the immediate vision is of somebody sat at a computer screen watching every move and click; that is simply not the case.

The fact that an Internet filter is in place to filter and monitor activity is of particular importance because you then have questions raised of morality such as, “It’s my human right to privacy”, “big brother is watching”, and others.

Why do we Filter and Monitor?

Schools filter Internet activity for two reasons:

We filter to ensure:

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavors to ensure the safety of those children and young people.

We monitor for assurance:

- (as much as possible) that no inappropriate or illegal activity has taken place.
- to add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding.

Managing Expectations

It is the expectations of the user that is particularly important; this will include school staff, pupils and parents/guardians of the pupils. Consent is not a requirement; however, we are required by law (Data Protection Act 1998) to make all reasonable efforts to inform users that we are monitoring them. By making reasonable efforts we will work “with” the pupils and parents, not just merely tell them.

Appendix 2

Letter to Parents:

Dear Parent/Carer,

Online Safety

Use of the Internet in school is a vital part of the education of your child. During the time your child is at our school we will make extensive use of the Internet in order to enhance their learning and provide facilities for research, learning and communication.

Whilst we do not allow children to peruse the internet unsupervised we recognise the potential for unsuitable, illegal or inappropriate websites to appear. As such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorises websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and Safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child, we will inform you of the circumstances.

Each school year we explain, in an age appropriate manner, the importance of Internet filtering to your child. Furthermore, we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please do not hesitate to contact us.

As acknowledgement please can you complete the reply slip below and read and complete the attached Acceptable ICT Use Policy with your child. We would appreciate it if these could be returned to school at your earliest convenience.

Yours sincerely,

Mrs L Cook
Headteacher



E-Safety

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that they have had the opportunity to voice their opinion, and to ask questions.

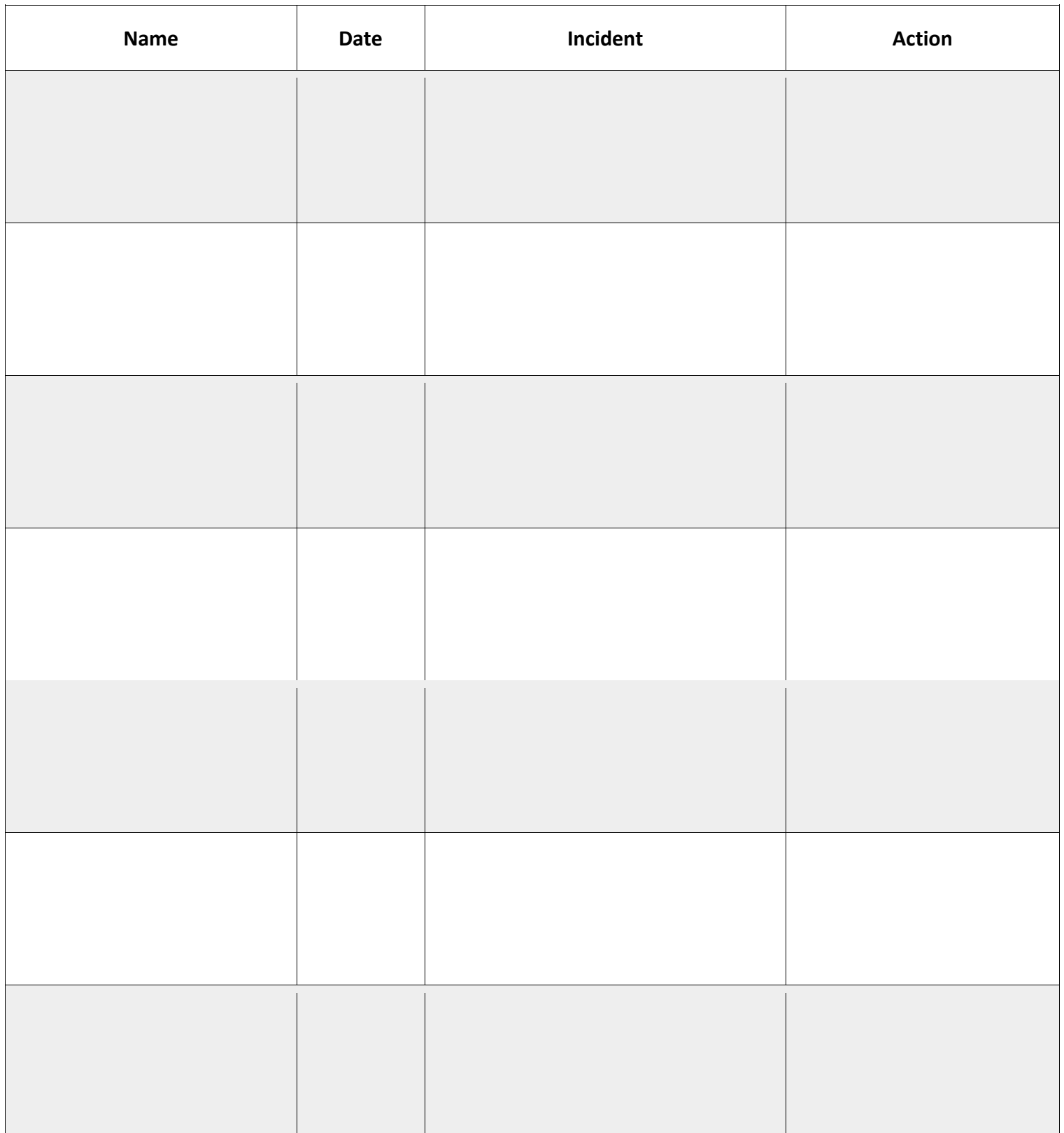
Name of Child: _____

Class: _____

Name of Parent/Carer: _____

Signature of Parent/Carer: _____

Date: _____



Appendix 3

Subsidiary Advice to Accompany the Online Safety Policy

Do we need social media channels?

With the way we communicate changing in this digital age. It is important that we as a school are able to engage with this to keep our parents informed of what is happening at school. However, we only want to have social media channels that are appropriate for our audience.

Five questions to ask before starting a new social media channel:

1. What is the main purpose of the proposed social media channel?
2. Can I reach my target audience with it?
3. Do I know which social media platforms best suit my core objective?
4. Do I have sufficient resources to keep it updated and monitored?
5. Am I likely to be posting regularly enough for the channel to have an impact on communication?

Usage and content principles

As a rule, social media users are warned not to post any content or information that they would not be prepared to say to the general public in other school communication. When posting on Branston Church of England Infant Academy social media platforms, consider the following:

- **Frequent** - Updates should be monthly or more frequent.
- **Useful** - Where possible, posts will include a link back to our school website.
- **Varied** - A wide range of media, photos, text and videos to retain interest.
- **Timely** - Posts will be relevant when posted or about upcoming events and opportunities.
- **Short** - Messages should be kept short, to the point and simple.
- **Accurate** - Our social media channels represent Branston Church of England Academy and its reputation. All spelling and grammar should be accurate. Text speak should not be used.
- **Corporate** - Social media is an extension of our school's website and brand.

Appendix 4

Personal Social Media Channels

While accounts of Branston Church of England Academy employees are their own business, it is still possible for the content of them to affect their professional standing and/or that of their employer.

To mitigate this risk, you may not include any reference to, or post comments about, Branston Church of England Academy, your job role, your colleagues, pupils, parents or partner organisations.

Management of allegations or disclosures

We will only be using the social media channels as a broadcasting system, therefore please be aware of the following issues:

- Posting a message on social media is viewed as a less formal manner of expression compared with speaking face-to-face or on a telephone and a young person may choose to utilise social media to make a disclosure or allegation.
- Any disclosure or allegation must be taken seriously, and immediate action taken to investigate.

Managing Grooming

Grooming is where, an individual, having communicated with a child or vulnerable adult on at least two occasions, then either meets them or travels with the intention of meeting them with the intention of committing an offence. Such conversations will be normally held by private messaging, however, should anything arouse your suspicions then contact the Designated Safeguarding Lead (Mrs Lianne Cook - Headteacher).

Appendix 5

Useful Links

CEOP

<https://www.ceop.police.uk/safety-centre/>

<https://www.thinkuknow.co.uk/>

<https://www.thinkuknow.co.uk/parents/>

NSPCC

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

Parentzone

<https://parentzone.org.uk/>

Safety Net Kids

<http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/>

UK Safer Internet

<https://www.saferinternet.org.uk/>

Internet Matters

<https://www.internetmatters.org/>



Online Safety Policy – Amendments

Date Actioned	Changes
April 2019	- Any reference to Governors/Governing Body/Local board amended to Local Council to reflect changes to school governance. - Reference to Miss Beverley Chambers changed to Headteacher due to staffing changes.
November 2021	Changed title to 'Online Safety Policy', which replaces 'E-Safety'. Changes to Headteacher name and also to E-Safety (Online Safety) Officer name. Additional details around the importance of online safety during Covid 19 pandemic response. Links added to KCSIE, Report on Sexual Abuse in Schools and Colleges June 2021, RSE Policy and school website online safety support.
March 2023	- Any reference to Local Council, updated to Academy Committee/Governors to reflect change to school governance. - Subject lead and E-Safety Officer details updated.
March 2025	Safe Use – Ipad section added.