Online Safety Policy 2020-21

University of Brighton Academies Trust

This policy was adopted on September 2020
This policy is due for review on September 2021

THE BAIRD PRIMARY ACADEMY

Key contacts

Role	Name	Contact details
Designated Safeguarding Lead (DSL)	Carly Welch (Principal)	safeguarding@thebairdprimaryacademy.org.uk 01424 425670
Deputy Designated Safeguarding Lead	Steph Jarvis Safeguarding Officer	safeguarding@thebairdprimaryacademy.org.uk 01424 425670
Deputy Designated Safeguarding Lead – e-safety	Roz Adie Computing Leader	safeguarding@thebairdprimaryacademy.org.uk 01424 425670
Nominated Local Board member for safeguarding and child	Rose Durban	chair@thebairdprimaryacademy.org.uk 01424 425670

1. Policy Aims

- This online safety policy has been adapted by The Baird Primary Academy, involving staff, pupils/students and parents/carers, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes account of the DfE statutory guidance Keeping Children Safe in Education 2020, Early Years and Foundation Stage and the East Sussex Safeguarding Children Partnership procedures.

- The purpose of The Baird's online safety policy is to:
  - Safeguard and protect all members of The Baird's community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns.

- The Baird identifies that the issues classified within online safety are considerable, but can be broadly 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.

2. Policy Scope

- The Baird believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils/students and staff are protected from potential harm online.
- The Baird identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- The Baird believes that pupils/students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the Board of Trustees, Local Board members, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the academy (collectively referred to as "staff" in this policy) as well as pupils/students, parents and carers.

- This policy applies to all access to the internet, cloud based apps and use of technology, including personal devices, or where pupils/students, staff or other individuals have been provided with Trust/academy issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.1 Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Academy Anti-Bullying Policy
- Acceptable Use Policies (AUP)
- Staff Code of Conduct
- Behaviour for Learning Policy
- Academy Child Protection and Safeguarding Policy
- Curriculum Policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection
- Photography and Image Sharing Policy
- Social Media Policies

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; this policy will be reviewed at least annually
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Principal will be informed of online safety concerns, as appropriate. All online safety concerns are logged in CPOMS and the Principal and Safeguarding Officer notified.
- The named Local Board member for safeguarding will report on, at least, an annual basis to the Local Board on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Carly Welch, Principal, has lead responsibility for online safety.
    - Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- The Baird recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Board of Trustees will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct and acceptable use policies, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place which enable technical staff to monitor the safety and security of our systems and networks; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).

4.2 The Principal will:

- Ensure that online safety is embedded within a progressive curriculum, which enables all pupils/students to develop an age-appropriate understanding of online safety.

- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.3 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the academy's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep pupils/students safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils/students with SEN and disabilities (SEND) face online.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the academy's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures. This will be supported by the Computing Leader.
- Report online safety concerns as appropriate.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (three times per year) with the Local Board Link member for safeguarding and provide information to the Principal to ensure that online safety concerns are reported to the Local Board via the Principal's report.

4.4 It is the responsibility of all members of staff to:

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

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.

- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.
- Keep their password confidential and safe

4.6 It is the responsibility of parents and carers to:

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

4.7 The Trust ICT team will:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the academy's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils/students

- The academy will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst pupils/students by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study. All information can be found in the Computing Protocol, saved in P:\Policies\Curriculum\Computing.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating pupils/students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching pupils/students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The academy will support pupils/students to read and understand the acceptable use policies in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing pupils/students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology with positive praise.

- Implementing appropriate peer education approaches, through the use of taught sessions or coaching.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking pupil/student voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Pupils/students

- The Baird recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The Baird will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils/students. All online safety education will be differentiated appropriately within the classroom using a range of approaches as detailed in our SEN Information Report.
- When implementing an appropriate online safety policy and curriculum The Baird will seek input from specialist staff as appropriate, including the SENCO, Looked After Children Designated Teacher.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the academy/Trust.

- Updates and training will be provided to staff during staff CPD sessions and this will be planned into the annual calendar. Training will also be provided on a needs-based basis to ensure that staff who are less confident receive increased training. This training will cover the potential risks posed to pupils/students (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the academy, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils/students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils/students, colleagues or other members of the community. These concerns are logged on CPOMS.

5.4 Awareness and engagement with parents and carers

- The Baird recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our Acceptable Use Agreements.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- The Baird recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the academy is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices. Any access to inappropriate content will be logged on CPOMS or emailed to safeguarding@thebairdprimaryacademy.org.uk

7. Safer Use of Technology

7.1 Classroom Use

- The Baird uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Purple Mash Learning Platform
    - Email through Purple Mash
    - Digital cameras, web cams and video cameras
    - Floor robots, data loggers, computer controlled technology
- All academy owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. For example apps will not be downloadable on iPads from pupil log ins; pupils log ins on laptops will be restricted as well.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The academy will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and pupils/students complies with copyright law and acknowledge the source of information.
- Supervision of pupils/students will be appropriate to their age and ability. (Amend as appropriate)
    - Early Years Foundation Stage and Key Stage 1
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
    - Key Stage 2
        - Pupils will use age-appropriate search engines and online tools.

- Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, pupils and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources, cloud based apps, or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- The University of Brighton Academies Trust have ensured that our academy has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The Trust is aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- The decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The Trust ICT Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils/students; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- Education broadband connectivity is provided through Schools Broadband.
- We use Netsweeper, which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The Trust ICT Team works with Netsweeper to ensure that our filtering policy is continually reviewed.
- If pupils discover unsuitable sites, they will be required to:
    - Turn off the screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL on CPOMS. They will also log this as an ICT job to be blocked.
    - The breach will be recorded on CPOMS as an e-safety concern and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Sussex Police or CEOP.
- Any concerns regarding filtering should be reported to the central ICT team through the ICT Helpdesk.

7.3.3 Monitoring

- We will appropriately monitor internet use on all academy owned or provided internet enabled devices. This is achieved by:
    - Supervision within classrooms
    - Monitoring content on Purple Mash – teachers have to approve any emails between pupils and approve content before it is posted.
    - Centralised monitoring and alert systems administered by the Trust ICT Team.
- If a concern is identified via monitoring we will respond in line with the academy Child Protection and Safeguarding policy. This includes reporting through CPOMS.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our Data Protection policy on the Trust website

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including: (Amend and add as appropriate)
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use. Any portable media provided by the academy will be encrypted.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on our network,
    - The appropriate use of user logins and passwords to access our network. Specific user logins and passwords will be enforced for all[1]
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found in Acceptable Use policies.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From Reception, all pupils are provided with their own unique username and private passwords to access Purple Mash and other web-based programmes that we use e.g. Times Table Rockstars; pupils are responsible for keeping their password private. To log on to the local area network, pupils have a class-based log in as this is not confidential
- We require all users to:
    - Use strong passwords for access into our system – these are a minimum of 10 characters and in line with Microsoft security recommendations
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

7.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our academy address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

[1] this should be in place for all except Early Years and Foundation Stage children and some pupils/students with SEND

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: Photography and Image Sharing Policy, Data Protection Policy, Acceptable Use Policies, Staff Code of Conduct, Academy Behaviour for Learning and Anti-Bullying Policies and Social Media policy.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including Acceptable Use Policies and the Code of Conduct and academy Behaviour for Learning Policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

- Members of the community will immediately inform the Computing Leader (Roz Adie) if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted. We therefore ask that staff consider the workload of other staff when sending emails / messages on Microsoft Teams and consider whether they are essential.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff – safeguarding@thebairdprimaryacademy.org.uk

7.8.1 Staff email

- The use of personal email addresses by staff for any official academy business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- When messaging parents, we ask that staff do this through the office@ email to prevent parents contacting staff directly via email.
- Staff can use the email function within Purple Mash to contact pupils directly regarding their learning.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

7.8.2 Pupil email

- Pupils will use provided email accounts for educational purposes. These are within Purple Mash. This is the only system that we use for pupil emails as teachers must approve pupil emails prior to sending.
- Pupils / parents and carers will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the academy.

7.9 Live Stream Lessons for Remote Learning

- Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function and it is this type of platform that will be used in the academy.
- When planning the use of live stream platforms within remote learning our academy will:
    - Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
    - Ensure that staff are trained to use the technology.
    - Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour for learning policy.

- Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

Protocols for the use of live streaming is included as Annexes A and B.

7.10 Management of Learning Platforms

- The Baird uses Purple Mash as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the LP.
- When staff and/or pupils leave the academy, their account will be disabled or transferred to their new establishment.
- Pupils and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - Inappropriate content will not be approved by the class teacher or Computing Leader
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A learner's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Pupils may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Children's Progress

- We use Target Tracker to track pupils' progress and share appropriate information with parents and carers.
- The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
  - Only academy issued devices will be used for apps that record and store pupils' personal details, attainment or photographs.
  - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils' personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft. This is through the Target Tracker encrypted log in key.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

Detailed information regarding the use of Social Media can be found in Acceptable Use Policies, Staff Code of Conduct and the Social Media Policy.

9. Use of Personal Devices and Mobile Phones

The Baird recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the academy.

9.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as code of conduct, anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of The Baird community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of The Baird community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as classrooms, playgrounds, toilets and any area where the pupils are present. Staff are only permitted to use their mobile phones in offices or staff rooms.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of The Baird community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.
- Further information on the use of personal devices is available in Acceptable Use policies and the Staff Code of Conduct.

9.5 Officially provided mobile phones and devices

- Mobile phones are provided for the Principal, the Facilities Manager and the Safeguarding Officer. There are also two mobile phones which are borrowed by staff for use on educational visits.
- Members of staff will be issued with a work phone number and email address, where contact with pupils/ or parents/ carers is required.
- Academy mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Academy mobile phones and devices will always be used in accordance with the acceptable use policy, staff code of conduct and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including, but not limited to, breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content. Detailed information can be found in the Academy Child Protection and safeguarding policy and procedure.

11.Useful Links

Pan-Sussex Safeguarding Children Partnership
www.sussexchildprotection.procedures.org.uk/

Sussex Police:
www.sussex.police.uk
For non-urgent Police contact 101 or 01273 470101
If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

There is a wealth of information available to support schools and parents/carers to keep children safe online. See Keeping Children Safe in Education 2020 (Annex C) for more resources.

12. Policy status and review

Written by:	Head of Governance and Admissions
Owner:	Executive Director of School Improvement
Status:	Approved
Approval date:	UoBAT – Board of Directors 10/12/15 HAT – Board of Directors 17/12/15 Merger editorial changes 1 September 2017 Chair of EAS – 23-09-2020
Review Date:	Annually

Annex A

Using Office 365 for remote learning

Guidance for Parents and Pupils

Dear parent/carer,

In response to COVID-19 and the possible local or national lockdowns, school closures or the need for isolation, the academy will continue to provide education. This may include remote streamed live lessons.

This use of technology is an important new development, and something we're really excited about. It means we can be confident teaching and learning can continue in an engaging way, and we hope act to minimise the educational impact of any further Covid-19 measures.

This new way of working will require all staff and pupils to think carefully about how they interact with one another virtually, in order to make sure learning is as safe and effective as it can be. In order to facilitate that, please find below is a list of expectations of all pupils taking part in live lessons. Please support us by ensuring that you read this guidance carefully and talk to your child about it.

- Please ensure your child joins their session in a shared space where you can monitor them. Ideally a living or dining room, they must not be joining Microsoft Teams from their bedroom.
- Please ensure your child is dressed appropriately, in clothing that may be worn on a home clothes day. No pyjamas.
- Be mindful that other pupils might see or hear anything in the background. Encourage your child to have a plain background, blur or set their background to an appropriate still picture.
- Your child may be asked to mute their microphone or turn their cameras off. This will be decided on a lesson by lesson basis; please follow the requests of the teachers.
- Your child must not instigate a call with any teachers.
- Your child is not permitted to record or screenshot sessions.
- Parents and children should not be using a student login to gain access to the contact details of teachers or other students.
- The University of Brighton Academy Trust will only use Microsoft Teams to deliver live lessons to your child.
- Pupil attendance will be recorded during these sessions.
- Parents and children must not use Microsoft Teams for anything other than the scheduled sessions/lessons. It is not to be used for any non-school related activity.
- When asked to participate via voice or text chat, your child should always use appropriate language making sure not to cause offence to others.
- Microsoft Teams is not to be used if your child wishes to 'chat' online to a friend outside of the scheduled sessions/lessons.
- Any misuse of any of our online services will be seen as a serious breach of the Academy's behaviour policy and referred directly to the Designated Safeguarding Leads, including the Principal.

If you do not consent for your child taking part in live streaming lessons, then please contact the academy immediately.

Annex B

Using Office 365 for remote learning

Guidance for Staff

1 Introduction

The University of Brighton Academies Trust provides Microsoft Office 365 access for staff and pupils across all Academies. This service offers exciting opportunities for remote learning that have not been previously possible. With opportunities there are new risks that this guide will help you manage.

The office 365 suite offers the following services: -

Microsoft Teams – Channels and Files (Video/Audio/Text Chat/Resources)	Allows staff to setup controlled Teams (groups of pupils) and collaborate in a number of ways. This includes the use of text chat, video and/or voice as well as the sharing of resources (including Word, Excel and PowerPoint documents)
Microsoft Stream	Allows staff to pre-record lesson content and upload it to the Academy website or share direct links to pupils to watch.
Microsoft Teams – assignments (This currently only applies to secondary sites)	Allows staff to set work for students to complete it and send it back for marking and feedback. This also includes quizzes and an online gradebook.

This document focuses on Microsoft Teams and sets out guidance to ensure you and your pupils remain safe whilst using the video/audio and text chat elements of this technology.

First and foremost, it is important to think of your Class Team as a traditional classroom. Any files that you upload can be viewed by all of the students. Any posts that are shared in the feed can also be viewed by all students. Therefore, do not upload or share anything that you would not normally do so in your classroom. Also, please note that Office documents will be editable by all users when you upload them. If you want to upload material that is simply for reference either set the file to 'view only' or upload a PDF version instead.

In terms of live streamed lesson:

As a staff member you can do the following easily during a session: -

- Choose which pupils you allow to enter your Team.
- Remove a pupil from a Team.
- Mute one or all pupils so they cannot speak.
- Delete unwanted posts or files that have been created by pupils.

By default, we have restricted pupils: -

- Students have no access to control the meeting including muting anyone other than themselves.
- They can post or comment within a class/meeting, but they cannot delete or edit the post or comment.
- Students accounts can also post comments and replies to posts in the main feed unless you have set your post to not accept replies. As above students cannot edit or delete their posts but you as the Team Owner can. Any comments or replies that do not adhere to the Academy code of conduct should be treated in the same way as they would be in a normal classroom.
- They can upload work for assignments that you have set as the teacher. They can see their individual feedback and grades but will not see the class gradebook.

Full training videos can be found in ICT services on the Office 365 Intranet

2 Protocols to keep you and your pupils safe

- When pupils join a live call, they should be asked to disable their webcam and only enable it when requested by a member of staff
- Staff can at any point raise a request with ICT service to permanently disable individual student webcam functionality if they feel the student has abused this feature.
- Two members of staff will be 'within the Team (in the same room at school, or if working remotely, in the video call) when conducting a live stream session with pupils. Both should be present before the pupils start to join.
- The second member of staff is there to provide a safeguard for both the pupils and the teacher, so does not need to be a curriculum specialist.
- The second member of staff could act additionally as technical/behaviour support, in terms of monitoring pupils' interactions and ensuring they are not using chat or other functions inappropriately.
- The second member of staff does not need to be present for the whole remote session but does need to gauge a view of safeguarding. It is recommended that they remain in the session for a minimum of 20 minutes.
- Sessions will be planned and scheduled for during school hours. If you need to run a session outside of normal school hours you will need to seek approval from a member of your academy leadership team.
- Parents will be contacted to advise that the session is taking place and they and the pupil should consent to abide to an acceptable use agreement covering issues such as not recording the session and being appropriately dressed etc.
- Only school contact numbers/emails will be used for communications and running the session i.e. staff should never issue their personal contact details.
- The only live streaming platforms approved is Microsoft Teams from the University of Brighton Academies Trust Office 365 tenant.
- Live streaming sessions should not be recorded.
- Live events should not occur with other members of your household present.
- Where inviting students as guests (via a link), ensure settings are set to 'admit from the lobby' therefore pupils cannot join without your knowledge. note - this is set by default.
- Staff should be aware of open applications including website tabs if using the screenshare functionality.
- Staff will dress professionally and choose a neutral background for their video stream.
- 1:1 video call sessions to support interventions with pupils such as mental health support or counselling will only be provided where they have been risk assessed and approved by SLT.
- Where the communication with an individual pupil does not require the confidentiality of a counselling session, there will be two adults involved; this will provide a safeguard for the adults and the pupil.
- These two adults will either be physically in the same room, with the second member of staff being referenced to the pupil so that they are aware, or, where staff are working remotely, they will both be within the Team of the meeting.
- In either case both adults will be present before pupils are admitted to the online session.
- At the end of the class, a member of staff should end the meeting to ensure all pupils are removed from the call rather than hang-up.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- Staff should read the Using Office 365 for remote learning guidance for pupils, so you fully understand the expectations of them during a session.
- All other school policies/practices should be followed, notably the safeguarding and pupil protection policy so should there be any welfare concerns about the pupil these should be brought to the attention of the DSL without delay.
- In most circumstances' attendance will need to be recorded :-

  Primary – Please continue to follow attendance coding guidance issued on 11.01.2021. There is a remote learning tracker available for each infant and primary academy. This spreadsheet will enable each academy to track and analyse engagement with remote learning. The tracker will support you to identify any missing children. Each tracker will calculate average hours of engagement for each year group and vulnerable cohorts. Links available on SharePoint. Please submit remote learning data centrally, as requested.

  Secondary – Please continue to follow attendance coding guidance issued on 11.01.2021. Create a tracking system that enables you calculate the average number of hours engagement and to identify

any missing children. The School Improvement and IT teams can support you with this. Face-to-face and live lessons, that run in sync with timetable lessons, can continue to be recorded on SIMS registers. Contact the Trust Attendance Manager/Interim Safeguarding and Welfare Lead for current attendance coding advice in secondary settings. Please submit remote learning data centrally, as requested.