Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Birchington CE Primary School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the Staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that Birchington CE Primary School systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Birchington CE Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies**.**

2. I understand that Birchington CE Primary School's Staff Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Birchington CE Primary School's Child Protection Policy, the Online Safety Policy and Staff Code of Conduct. This includes any remote learning.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Birchington CE Primary School ethos, Birchington CE Primary School staff Behaviour and Safeguarding policies, national and local education and Child Protection & Safeguarding guidance, and the law.

Use of Birchington CE Primary School Devices and Systems

1. I will only use the equipment and internet services provided to me by the Birchington CE Primary School for example Birchington CE Primary School provided laptops, tablets, mobile phones and internet access, when working with learners. Explicit permission must be sought from the Headteacher for the use of any type of personal mobile device within the working day.

2. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Personal use of Birchington CE Primary School's IT systems and/or devices by staff, visitors and volunteers is not allowed.

3. Where I deliver or support remote learning, I will comply with the school's remote learning AUP.

Data and System Security

1. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

2. I will use a 'strong' password to access Birchington CE Primary School systems. *(A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).*

3. I will protect the devices in my care from unapproved access, by logging off or locking devices when not in use, or theft by not leaving devices unsupervised in public spaces or in my car

4. I will respect Birchington CE Primary School system security and will not disclose my password or security information to others.

5. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT Network Manager.

6. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT Network Manager.

7. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the Birchington CE Primary School information security policies.

8. All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

9. Any data being removed from the Birchington CE Primary School site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the Birchington CE Primary School. Staff are not permitted to use data sticks unless explicit permission has been granted by the Headteacher.

10. I will only use school provided devices to access any school related work including using my school provided email address account. The school's approved/provided VPN (Virtual Provided Network) is only accessible via a school provided laptop, and this is the only way staff can login to the school network when not in school. Some staff's laptops have direct remote secure connections to their work computers.

11. I will not keep documents which contain Birchington CE Primary School related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. I will not use my school email address as my profile on any internet browser that is not accessed on a school device.

12. I will not store any personal information on the Birchington CE Primary School IT system, including Birchington CE Primary School laptops or similar device issued to members of staff, that is unrelated to Birchington CE Primary School activities, such as personal photographs, files or financial information.

13. I will ensure that Birchington CE Primary School owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

14. I will not attempt to bypass any filtering and/or security systems put in place by Birchington CE Primary School.

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the IT Network Manger – Mr Matt Horsburgh as soon as possible.

16. If I have lost any Birchington CE Primary School related documents or files, I will report this to the IT Network Manager and the Data Protection Lead, Mr Jonathan Forwood, as soon as possible.

17. Any images or videos of learners will only be used as stated in the Birchington CE Primary School camera and Image Usage Agreement.

18. I understand images of learners must always be appropriate and should only be taken with Birchington CE Primary School provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

1. I am aware of the expectation relating to safe technology use in the classroom, safe remote learning, and other working spaces, including appropriate supervision of learners, as outlined in the Birchington CE Primary School Online Safety Policy and Child Protection Policy.

2. I have read and understood the Birchington CE Primary School Online Safety Policy which covers expectations for learners regarding mobile technology and social media.

3. I will promote Online Safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

    - exploring Online Safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site

    - creating a safe environment where learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online

    - involving the Designated Safeguarding Lead, Mrs Louise Wilson, or Deputy DSLs as part of planning Online Safety lessons or activities to ensure support is in place for any learners who may be impacted by the content

    - make informed decisions to ensure any Online Safety resources used with learners is appropriate

4. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the Lead DSL or Deputy DSLs in line with the Birchington CE Primary School Online Safety and Child Protection & Safeguarding policy.

5. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Personal mobile and smart technology

I will ensure that my use of personal mobile and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff Behaviour policy, Code of Conduct and the Birchington CEP School's 'Mobile and Smart Technology policy' and the law.

Online communication, including use of social media

1. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the Child Protection and Online Safety policies, Staff Code of Conduct, Birchington CEP School's Social Media Policy and the law.

2. As outlined in the staff Code of Conduct and school social media policy:

    - I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to children/pupils/students, staff, school business or parents/carers on social media.

3. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

    - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a Birchington CE Primary School email address, user accounts or telephone numbers.
    - I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
    - If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my line manager and Louise Wilson, Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the Headteacher and Lead DSL.

Policy Concerns

1. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

2. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

3. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Birchington CE Primary School into disrepute.

4. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to a DSL in line with the school's Child Protection policy.

5. I will report concerns about the welfare, safety, or behaviour of staff online to the Headteacher/Lead DSL, in line with the school's Child Protection policy.

Policy Compliance and Breaches

6. If I have any queries or questions regarding safe and professional practise online either in Birchington CE Primary School or off site, I will raise them with the Headteacher/Lead DSL.

7. I understand that the Birchington CE Primary School may exercise its right to monitor the use of information systems, including internet access and the interception of messages/emails on our systems, to monitor policy compliance and to ensure the safety of pupils and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

8. I understand that if the Birchington CE Primary School believe that unauthorised and/or inappropriate use of Birchington CE Primary School systems or devices is taking place, the Birchington CE Primary School may invoke its disciplinary action as outlined in the Staff Code of Conduct and KCC Discipline Procedures.

9. I understand that if the Birchington CE Primary School believe that unprofessional or inappropriate online activity, including behaviour which could bring the Birchington CE Primary School into disrepute, is taking place online, the Birchington CE Primary School may invoke its disciplinary procedures as outlined in the Staff Code of Conduct and KCC Discipline Procedures.

10. I understand that if Birchington CE Primary School suspects criminal offences have occurred, the police will be informed.

School Provided Leader/Office/Site/IT/Pastoral Manager Mobile Phones

The following section is just for those members of staff who have been provided with a smart phone.

Use of Phones

1. No school provided mobile phone is to be used for any personal reasons.

2. Work provided phones/phone numbers are provided by the setting for certain members of staff in order that they can perform their job role. These include Leaders, Office Manager, Site Staff, Network Manager and FLO.

3. These phones can be used for phone calls, text messages and Whatsapp calls/messages in relation to the job role of the user.

4. No apps are to be downloaded, apart from Whatsapp and Microsoft Authenticator except if permission has been sought from the Headteacher.

5. If any staff need to have conversations with children they must be held with a parent/carer in attendance and staff must ask that parents/carers put their phone on speaker in order to facilitate this. Typing 141 in front of the number will ensure your number is withheld. You must delete parent/carer numbers from your call log at the end of each day (with the exception of the FLO).

6. Contact is only to be made with parent/carers contact details and not with children's own mobile phones. If for any reason a child contacts a teacher on their school phone, the teacher must stop the contact immediately and report this to a DSL.

Security and Safety of Phones

7. School provided mobile phones will be suitably protected via a passcode/password/pin and must only be accessed or used by the member of staff to whom the phone has been given. Matt Horsburgh – Network Manager – will have the list of all passcodes. This must not be changed without the Headteacher's permission and with the knowledge of the Network Manager

8. No phone numbers are to be added to the phone except by Matt Horsburgh – Network Manager.

9. All school provided mobile phones must be kept with the individual at all times during the day so other staff can contact you if necessary. At night it must be stored in a safe place/high cupboard or a locked cupboard/room.

10. If, for any reason, the phone needs to be taken off site then the user must get the permission of the Headteacher.

11. The phone's camera may be used if it is necessary for the member of staff to fulfil their job role. No photos of children are to be taken on these phones.

12. All staff must take precautions to keep the mobile phone free from damage/loss. Any damage/loss to a school provided mobile phone must be reported to the Headteacher immediately.

13. All school provided mobile phones will be signed for when given out and when returned.

Policy Adherence

14. Where staff are using school provided mobile phones, they will be informed prior to use that activity may be monitored for safeguarding reasons and to ensure policy compliance.

15. School mobile phones will always be used in accordance with this AUP, Remote Learning AUP, and the Child Protection, Online Safety, and IT Polices

16. If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.

17. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

18. If a member of staff is asked to hand in their mobile phone they will do so immediately. If a member of staff leaves the mobile will be handed back in along with their laptop, key fob etc.

19. The mobile phone remains the property of Birchington CEP School.

School Provided Teacher/Medical Mobile Phones

The following section is just for those members of staff who have been provided with a non-smart phone.

Use of Phones

1. No school provided mobile phone is to be used for any personal reasons.

2. Work provided phones/phone numbers are provided by the setting for teachers**,** in addition to their work email address, where contact with learners or parents/carers is required. Contact with the parents/carers by phone will be by phone call only.

3. Any conversations with children must be held with a parent/carer in attendance and staff must ask that parents/carers put their phone on speaker in order to facilitate this.

4. Contact is only to be made with parent/carers contact details and not with children's own mobile phones. A teacher MUST input 141 prior to inputting the phone number to ensure their number is withheld.

5. If for any reason a child contacts a teacher on their school phone, the teacher must stop the contact immediately and report this to a DSL. This situation should never happen if teachers ensure they input 141 before any calls (see 4 above)

6. Teachers may also use these phones to contact other teachers within the school, other members of staff with school mobile phones or phoning the school office.

7. A work provided mobile phone may also be issued to other members of staff if they need it to make immediate contact with a parent for critical medical reasons. This phone is only to be used to contact the parent/carer of the child that has the medical need. This phone is to remain in school at all times with the adult who has been issued the phone and kept in a safe place/high cupboard or (if possible) a locked cupboard/room.

Security and Safety of Phones

8. School provided mobile phones are lockable, with the press of 2 buttons, and must be locked when not in use.

9. No phone numbers are to be added to the phone except by Matt Horsburgh – Network Manager.

10. The phone's contact log must be cleared at the end of the school day.

11. Teacher not self-isolating: all school provided mobile phones must be kept with the individual at all times during the day or stored in a safe place/high cupboard etc. At night it must be stored in a safe place/high cupboard or (if possible) a locked cupboard/room.

12. Teacher self-isolating with no symptoms: school mobile phones will be needed at home. In these circumstances the phone will be delivered to your home for you to use.

13. The phone's camera will not be used for any purpose.

14. All staff must take precautions to keep the mobile phone free from damage/loss. Any damage/loss to a school provided mobile phone must be reported to the Headteacher immediately.

15. All school provided mobile phones will be signed for when given out and when returned.

Access to Parent/Carer Phone Numbers

16. Teacher accessible SIMS, on classroom computers, will have the contact details of parents/carers for the class teacher to access. There will be no access to medical information.

17. If a teacher is self-isolating at home, the school will provide the parent/carers' contact details to the teacher via their work email.

Policy Adherence

18. Where staff are using school provided mobile phones, they will be informed prior to use that activity may be monitored for safeguarding reasons and to ensure policy compliance.

19. School mobile phones will always be used in accordance with this AUP, Remote Learning AUP, and the Child Protection, Online Safety, and IT Polices

20. If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.

21. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

22. If a member of staff is asked to hand in their mobile phone they will do so immediately. If a member of staff leaves the mobile will be handed back in along with their laptop, key fob etc.

23. The mobile phone remains the property of Birchington CEP School.

I have read, understood and agreed to comply with Birchington CE Primary School's Staff AUP (including the school provided mobile phone sections if applicable) when using the internet and other associated technologies, both on and off site.

Name of Staff Member: ……

Signed: …….....

Date (DD-MM-YY)……...