# BRIDGE & PATRIXBOURNE CEP SCHOOL

# ACCEPTABLE USE OF TECHNOLOGY (STAFF) POLICY & PROCEDURE

Bridge & Patrixbourne Church of England Primary School is a welcoming and nurturing community which promotes: ***creativity*** (developing our gifts); ***excellence*** (being the best we can be) and ***resilience*** (learning from our experiences). The school provides opportunities which enable everyone to flourish and grow within the love of God.

> *I am the vine, you are the branches. If you remain in me and I in you, you will bear much fruit. Without me, you can do nothing.*
>
> **John 15:5**

## Key Personnel

**Headteacher:** James Tibbles

**Chair of T&L Team:** Catherine Hellman

## Key Dates

**Ratified by T&L:**

**Date of next review:**

# Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Bridge & Patrixbourne CEP 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 Bridge & Patrixbourne CEP School expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that 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

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 Bridge & Patrixbourne CEP 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**.**

I understand that Bridge & Patrixbourne CEP School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct and remote learning AUP.

I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

## Use of School Devices and Systems

I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones, and internet access, when working with learners.

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. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

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

## Data and System Security

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.

I will use a ‘strong’ password to access school systems.

I will protect the devices in my care from unapproved access or theft.

I will respect school system security and will not disclose my password or security information to others.

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 Headteacher.

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

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

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.

Any data being removed from the 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 school.

I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school approved VPN.

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

I will ensure that 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.

I will not attempt to bypass any filtering and/or security systems put in place by the school.

If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Headteacher as soon as possible.

If I have lost any school related documents or files, I will report this to the Headteacher as soon as possible.

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

## Classroom Practice

I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the child protection policy.

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.
- 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 (DSL) (James Tibbles) or a deputy (Michael Taylor, Carla Long, Morny Starling) 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.

I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school child protection policies.

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.

## Use of Social Media and Mobile Technology

I have read and understood the school code of conduct which covers expectations regarding staff use of mobile technology and social media.

I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the mobile technology (link) policy.

I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.

I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the code of conduct and the law.

My electronic communications with current and past learners 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 school email address, user account or telephone number.

I will not share any personal contact information or details with learners, 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 learners and/or parents/carers.

If I am approached online by a learner or parents/carer, I will not respond and will report the communication to my line manager and James Tibbles (Designated Safeguarding Lead).

Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the Headteacher.

If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Headteacher.

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.

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

I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

## Policy Compliance

I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

## Policy Breaches or Concerns

I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school child protection policy.

I will report concerns about the welfare, safety, or behaviour of staff to the headteacher, in line with the allegations against staff policy.

I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the code of conduct.

I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the code of conduct.

I understand that if the school suspects criminal offences have occurred, the police will be informed.

**I have read, understood and agreed to comply with Bridge & Patrixbourne CEP School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.**

Name of staff member: ……

Signed: ……..

Date (DDMMYY)……..