



Baldwins Gate CE Primary School

Staff Acceptable Use Policy

Date of review	May 2022
Chair of Governors	Fiona Boulton
Headteacher	Leanne Lowndes
Date of next review	May 2023

The School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

Staff Acceptable Use Policy - ICT (AUP)

At Baldwins Gate CE Primary School we ask all adults involved in the life of the school to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). This AUP is reviewed annually and school staff will be asked to sign it upon entry to the school and every time changes are made.

All staff, governors and volunteers have particular legal/professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy, which is available on the school's website.

All staff, governors and volunteers should read Baldwins Gate Primary School's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to the headteacher or another member of the school's senior leadership team. Online Safety is considered a safeguarding area. Concerns should be reported in the same way as other Safeguarding concerns.

Appendix 1 of this policy outlines further information on email use and email etiquette.

Appendix 2 of this policy outlines further information on internet use.

By signing the staff acceptable use policy you are agreeing to:

- having read and understood Baldwins Gate Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Online Safety Lead (if by a child) or Headteacher (if by an adult).
- I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
- I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
- Photography material/video footage that includes pupils should not be taken or stored on personal devices.
- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy.
- Details on social media behaviour, is stated in the Social Media Policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
- I understand the importance of upholding my online reputation, that of the school and of the teaching profession), and I will do nothing to impair either.
- I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.

- I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for.
- I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the head teacher if I suspect a breach.
- I will not store school-related data on personal devices, storage or cloud platforms. USB keys or external hard drives must be password protected.
- I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
- I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring. I will look after devices loaned to me,
- I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I understand and support the commitments made by pupil, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
- I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might think are unimportant – I understand the principle of ‘safeguarding as a jigsaw’ where my concern might complete the picture, but only if I tell somebody. I have read the sections on handling incidents and concerns about a child in general, sexting, bullying, sexual violence and harassment, misuse of technology and social media.
- I understand that breach of this AUP and/or of the school’s full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
- I understand that I am given appropriate access to my role and relationship within the school. If I discover my settings are incorrect, I will inform the school’s senior leadership team immediately – I will not deliberately attempt to access content that I do not require in order to fulfil my role with the school.



Baldwins Gate CE (VC) Primary School

Staff Acceptable Use Policy (AUP)

By signing this document, you confirm that you have read, understood and agreed to the points addressed.

I understand that it is my responsibility to ensure I remain up to date and understand the school's most recent online safety/safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Name:	
Role:	
Signature:	
Date:	

Appendix 1

Email use

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of email within the school. These policies are in addition to those already set out in sections that apply across the entire range of the school's computing and telecommunications facilities.

The most common method of virus transmission into computing systems is via email. You should always be suspicious of attachments that arrive unexpectedly even if they appear to come from someone you know. If in doubt, don't open the message and contact Mr Ahearne immediately who will contact our ICT support services.

You should be aware that email messages carry the same weight in court as printed letters on school letterhead. Thus, ill-considered messages could have serious repercussions. For example, you may be held to account for making defamatory remarks via email. A defamatory statement is one that tends to damage the reputation of another individual or organisation.

You must not participate in office gossip and/or spreading rumours over the email system about clients, customers, staff, contractors, competitors – in short, everyone. Even if it may seem innocent to you, it may give rise to liability for defamation by both you and the school. The school by its very nature gives a great deal of advice to a wide range of people – that advice is obviously given through its staff. You will know whether or not it is part of your duties to give advice via email and the extent of your authority to do so. If you are acting within the normal course of your duties and your expertise, and you act in good faith without malice or capriciousness, then you will be protected even if your advice proves to be wrong. However, if you act outside your competence or outside your authority then again you may be liable for any harmful consequences of your actions. If you are asked to give advice in email, and you are unsure whether or not you are competent to give it, then don't - at least not without seeking advice yourself from senior leadership.

Do not enter into contractual commitments by email without legal advice. Email is capable of forming or varying a contract in just the same way as a written communication. Because of the perceived informality of email, there is the danger of contracts being inadvertently formed by employees, to which the school is then bound. You must comply with the following rules before entering into contracts by email:

- You must obtain authorisation, from senior leadership or Governors, before negotiating contracts by email. You must take advice from the leadership team or Governors before entering into contractual commitments.
- You must include the statement "subject to contract" in all emails if you conduct contractual negotiations via email until such time as it is intended that a binding contract should come into existence.
- You must be satisfied of the legal identity of the other contracting party before entering into a binding contract via email if given the authority to do so.

Email Etiquette

In addition to the above rules, the following guidelines should be followed when using the email system:

- Always maintain a professional image. Ensure the style, tone and content of emails is appropriate.
- Do not use email for urgent messages. Use the telephone. It should be noted that the delivery and integrity of email cannot be guaranteed.
- Respond to emails in a timely and professional manner. Always try to acknowledge receipt of emails requiring responses even if you cannot reply fully straightaway.
- Send emails only to those recipients/groups for whom the message is intended.
- Ensure the subject matter is clearly indicated in the heading.
- Try to use plain text in emails. Fonts, underline, colour, graphics and tables not only add to the message size, slow systems down and may adversely affect delivery times but may also be lost in external emails.
- Avoid sending trivial messages, jokes, gossip or adverts by email.
- Identify your contact details in emails.
- Re-read and spell check messages prior to sending to ensure accuracy and clarity.
- Read and delete emails regularly.

Email messages can be impersonal and/or misinterpreted so when sending an email consider whether it is the most effective method of communicating in that situation.

Appendix 2

Internet Use

You should ensure you are aware of and comply with the rules in this section, which specifically address the use of the school's internet facilities. These policies are in addition to those already set out in sections that apply across the entire range of the School's computing systems. The school encourages authorised staff to access the Internet during working hours, when direct work-related benefits can result. However, there are limits to personal use of the internet.

You should note:

- Different access for different types of personnel may be given.
- The school reserves the right to block access to certain Internet sites.
- Internet sites that are cost related or have cost implications in their terms of access must not be subscribed to without the prior authority of the head teacher.
- Without prior approval from the Headteacher in consultation with the Computing Lead, you may not download software or files from the internet for use on the school's systems.
- Any such software or files that are approved for download via the internet become the property of the school and may be used only in ways that are stipulated by their licences or copyrights.
- Excessive personal use of the Internet during or outside business hours is not allowed.

Do not download, store, reproduce or distribute documents, pictures, logos, music or works of others without the owner's permission as this may infringe copyright laws. If you download articles and other materials from the Internet, you must remember that you need permission from the author before using such information for business purposes.