Blessed Dominic Catholic Primary School

“Love Learn Believe”

Staff, Volunteers, Governors & Contractors Acceptable Use Policy Agreement

Date of policy September 2023
Next Review: September 2024

Mission Statement

At Blessed Dominic Catholic Primary School, we pride ourselves on being a culturally diverse family. We seek to instil, in every child that we nurture, the joy and wonder of learning.

As we journey together with Christ, we develop children's resilience, intellectual curiosity and creativity through our positive learning behaviours. We nurture and cherish the unique talents of all, to empower them to flourish and grow into life-long learners.

Our mission is to show love, promote learning and belief in God our Father.

LOVE – LEARN- BELIEVE

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

What is an AUP?
We ask all children, young people and adults involved in the life of Blessed Dominic Catholic Primary 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 I will be asked to sign it upon entry to the school and every time changes are made

Why do we need an AUP?
All staff (including support 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 https://www.blesseddominicprimary.co.uk/our-school/policies .

Where can I find out more?
All staff, governors and volunteers should read Blessed Dominic Catholic Primary School's full Online Safety Policy https://www.blesseddominicprimary.co.uk/our-school/policies 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 a member of the Senior Leadership team or the Computing Lead.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

Also covers school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

Blessed Dominic Catholic Primary School regularly reviews and updates all AUP documents to ensure that they are consistent with the school E-Safety Policy.

What am I agreeing to?

- **For Staff and Governors:**

- I have read and understood Blessed Dominic Catholic Primary School 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 Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult).

- I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)

- I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom. understand the sections on.

- I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.

- **During remote learning:**
    - Please refer to Appendix 2: To keep kids safe online during school closures
    - **I will not behave any differently** towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

    - **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.

    - **I will not take secret recordings or screenshots** of myself or pupils during live lessons.

    - **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.

- **I will complete the issue log for live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students.

- I will take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment - and maintain an attitude of 'it could happen here'
- I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

- I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

- When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).

- I will follow best-practice pedagogy for online-safety education, avoiding scaring and other unhelpful prevention methods.

- I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness. I will flag any concerns about overblocking to the DSL.

- I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.

- I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

- I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the **RSHE curriculum,** as well as safeguarding considerations when supporting pupils remotely.

- I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

- I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE 2023, now led by the DSL. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.

- 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 social media,
    - e.g. by not sharing other's images or details without permission;
        - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

- 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. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.

- Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety 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, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this https://static.lgfl.net/LgflNet/downloads/online-safety/LGfL-OS-Advice-Online-Reputation-Managment-for-Schools.pdf guidance for schools and in Blessed Dominic Catholic Primary School's social media policy/guidance https://www.blesseddominicprimary.co.uk/our-school/policies .

- I agree to adhere to all provisions of the school Data Protection Policy [https://www.blesseddominicprimary.co.uk/our-school/policies]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 SLT if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

- I will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

- I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and 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 pupils/students, 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 safeguarding and online-safety policies for reporting incident: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I

have read the sections on handing incidents and concerns about a child in general, sexting, up skirting, 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.

Appendix 1

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read 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.

Signature ..... Date.....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date .....

Full Name ..... (printed)

Appendix 2:

LGfL DigiSafe keeping children safe

SIX TOP TIPS

To Keep Primary Kids Safe Online During School Closure

Children are bound to spend lots more time on devices during school closure. DON'T FEEL BAD ABOUT IT – lots will be schoolwork or catching up with friends. But there are ways to keep them safe, healthy and happy.

Don't worry about screen time; aim for screen quality

Scrolling through social media isn't the same as making a film or story, or Skyping Grandma. Use the Children's Commissioner's 'Digital Five A Day' to plan or review each day together.

Check the safety settings are turned on

Whether it's your home internet, mobile devices, consoles, apps or games, there are lots of settings to make them safer. The key ones are – can they chat to strangers, can they video chat or 'go live', are their posts public? Internet Matters has hundreds of guides to parental controls.

Get your children to show you their apps and games

You don't need to know all about the latest app or game, but if your child shows you what they are doing and with whom, you'll probably see if it's appropriate or not. Remember 18 games are not more advanced – they are harmful to children! For parent guides to apps, including recommendations for kidsafe apps and video platforms, search for Common Sense Media or NSPCC's NetAware. And why not download the BBC Own It app?

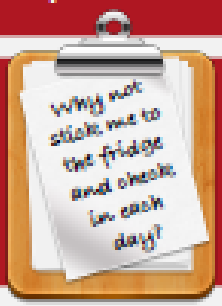
Don't try to hide the news about coronavirus

If you don't talk about it, your children might read inappropriate pages, believe scare stories or simply catastrophise in their heads. Why not watch Newsround together and talk about how they feel – there is guidance from Childline to help you.

Remind them of key online safety principles

There are too many to list, but remember human behaviour is the same online and offline. Remind your children to be a good friend, to ask for help if they are worried or if someone is mean, not to get undressed on camera and most important of all.... if somebody tells them not to tell or ask for help because it's too late or they will get in trouble, THAT'S A LIE!

If you aren't sure, ASK!



Your school may be able to give you advice, but there are plenty of other places to ask for help as a parent or a child, whether it is advice or help to fix something. Lots of sites are listed at reporting.lgfl.net, including ones to tell your kids about (they might not want to talk to you in the first instance).

You can find anything above by just googling it, or follow us @LGfLDigiSafe on Twitter or Facebook where we regularly share these resources