Mobile Phones and Devices Policy (Pupils, Staff and Visitors)

Date	Review Date	Coordinator	Nominated Governor
March 2024	March 2027	Krista Green	Micky Dixon

Introduction and aims

At Llangewydd, we recognise that mobile phones and devices that connect to the internet are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

Our policy aims to:

- Promote, and set an example for, safe and responsible phone/device use
- Set clear guidelines for the use of mobile phones/devices for pupils, staff, parents and volunteers
- Support the school's other policies, especially those related to child protection and behaviour

This policy also aims to address some of the challenges posed by mobile phones and devices in school, such as:

- Risks to child protection
- Data protection issues
- Potential for lesson disruption
- Risk of theft, loss, or damage
- Appropriate use of technology in the classroom

Roles and responsibilities

Staff

- All staff (including teachers, support staff, and supply staff) are responsible for enforcing this policy.
- All staff are being protected by the procedures in this policy.
- Pupils must secure their phones/devices as much as possible, including using passwords or pin codes to protect accessto the phone's functions.
- Staff will check that pupils' phones are switched off during the school day.
- Staff must also secure their personal phones/devices, as well as any work phone provided to them. Failure by staff to do socould result in data breaches.
- Volunteers, or anyone else otherwise engaged by the school will be made aware of this policy through theinformation given at Reception.
- Staff need to report any breaches of this policy to the Headteacher.
- Staff must read, sign and date the 'Staff and Volunteer Acceptable Use of ICT Policy' as well as the 'PROTOCOL FOR THE USE OF SOCIAL MEDIA document' at the start of each academic year (or when starting their role)

Use of mobile phones by staff

Personal mobile phones

- Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their mobile devices while children are present/during contact time. Staff keeping their phone with them during contact timesmust ensure their phone is on silent and in a secure place (e.g. locker/bag).
- Use of personal mobile phones is restricted to non-contact time, and to areas of the school where pupils

are not present such as the staff room and offices.

- In circumstances where immediate contact is needed, then staff should let family/ their child's school know to call Reception as personal phones will not be accessed during the school day.
- Staff members will not use their own personal phones to contact parents. If the staff member is at home (for example, PPA) then they can use their personal phones to contact parents, however their mobile number must be hidden.
- The Headteacher will decide on a case-by-case basis whether to allow for special arrangements. If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact.

Data protection

See the schools' policies on Data Protection

- Staff must not use their personal mobile phones to process personal data, or any other confidential school information.
- Staff can use school iPods, iPads/ cameras to take pictures – not personal devices.
- Staff can access website programs that access data on external servers such as My Concern or Sims.
- Staff must secure their phones as much as possible, including using passwords or pin codes to protect access to the phone's functions. Staff must also secure any work phone provided to them. Failure by staff to do so could result in data breaches.

Safeguarding

- Staff must not give their personal contact details to parents or pupils, including connecting through social media and messaging apps.
- Staff must not contact children on the child's personal devices, only ever contacting them through their parent/carer should this be required/necessary to do so.
- Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents or pupils.
- Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil.
- If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

Using personal mobiles for work purposes

› *See the school's policies on educational visits.*

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency
- Supervising off-site
- Residentials

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil.

- Refrain from using their phones to contact parents. If necessary, contact must be made via the school office or visiting venue phone.

Work phones

Some members of staff are provided with a mobile phone by the school for work purposes.

Only authorised staff are permitted to use school phones and access to the phone must not be provided to anyone without authorisation.

Staff must:

- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet.
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line withour staff code of conduct.

Sanctions

- Staff that fail to adhere to this policy may face disciplinary action.

Use of mobile devices by pupils

Pupils are allowed to bring a mobile to school, though must hand it in upon arrival for the teacher to lock away. The phone will then be given back to the pupil at the end of the school day. This includes:

- Pupils travelling to and from school by themselves.
- Pupils travelling by car by their parents/carers (preferably left with their parent when reaching school).
- Pupils travelling to school via LA Transport.
- Young carers who need to be contactable.
- Personal phones/ tablets that are internet enabled and have cameras are not allowed on school trips, during the day nor during afternoon clubs (specific personal circumstances will be considered on a risk-assessed basis).
- Camera watch devices must not be worn in school unless the cameras/video option is disabled.

Sanctions

School is permitted to confiscate phones from pupils.

- Sch~~ool staff have the ri~~ght to request to check pupils' mobile devices if a safeguarding issue arises within school.
- If devices are confiscated, parents/carers will be contacted to collect the phone/device.
- Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

- Sexting
- Inappropriate videos/photos being shared
- Threats of violence or assault
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity,

religiousbeliefs or sexual orientation

Use of mobile phones by parents, volunteers and visitors

Parents, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils on school grounds or school trips or when working with pupils.
- Not posting any images/data about the school on social media without consent.
- Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents, unless in a medical emergency.
- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

Parents or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones.

Parents must use the school office as the first point of contact if they need to get in touch with their child during the schoolday. They must not try to contact their child on his/her personal mobile during the school day.

Loss, theft or damage

- Pupils bringing phones to school must ensure that phones are handed in to the teacher to avoid loss, theft or damage.
- Pupils must secure their phones as much as possible, including using passwords or pin codes to protect access to the phone's functions.
- The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.
- Confiscated phones will be stored in the school office in a secure location until collected.
- Lost phones should be returned to Reception. The school will then attempt to contact the owner.

Headteacher:	Krista Green	**Date:**	March 2024
Chair of Governing Body:	Micky Dixon	**Date:**	March 2024

Appendix 1

Llangewydd Junior School

Staff and Volunteer Acceptable Use of ICT Policy.

2023-24

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, school email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, websire, blogs, VLE etc) out of school, and to the transfer of personal data (digital or paper based) off the school premises.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use during times when I am not on duty and not in the presence of school students (as stated within the policies and rules set down by the school).
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the ICT coordinator, safeguarding officer or other member of the eSafety group.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school during times when I am not on duty and not in the presence of school students, in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks

attached to using their personal email addresses / mobile phones / social networking sites for such communications)

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a computer, or store programmes on a computer, nor will I try to alter computer settings without consulting the ICT coordinator or engineer.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential (in a password protected location), except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school* :

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Appendix 2

Bridgend County Borough Council
Cyngor Bwrdeistref Sirol Pen-y-bont ar Ogwr
www.bridgend.gov.uk

PROTOCOL FOR THE USE OF SOCIAL MEDIA 2023/24

1. Introduction

1.1 Social media is the term given to online media/websites that are based on user-generated content and participation. Social media can fall under the following categories: blogs, forums, podcasts, wikis, networks and other online communities.

1.2 As part of our communications and engagement strategy, the school is committed to engaging with citizens and other interested parties in an effective and transparent way. Social media allows the council to develop two-way, real-time communications with its various stakeholders. If managed appropriately the use of social media as a communications tool for the school can be very helpful.

1.3 Other service areas across the authority have a presence on different platforms such as Twitter, Facebook, Linked-In and YouTube. These accounts are managed by the Headteacher.

1.4 Social media is also a key part of the council's ICT strategy. This social media protocol has been developed in line with the council's ICT protocols and the ICT Code of Practise which is applicable to all council staff.

1.5 Corporately the council has developed a 'Bridgend County Borough Council, social media and you' protocol which is available on the BCBC website. The aim of this is to be clear about how the council will engage with users and to manage expectations.

1.6 While the school respects the privacy and legal rights of employees, actions in or outside work that affect performance, the work of others, or the school/council's interests or reputation need to be considered as part of this social media protocol. Therefore this protocol covers employee responsibilities when using social media either for personal or professional use.

2. Using social media for personal use (during and outside of working hours)

2.1 When creating your own profile on a social media platform, it is important to remember that if you state you are an employee of the school, you are declaring yourself a representative of the school and must therefore act appropriately to avoid having a negative impact on yourself, the school and its reputation.

2.2 To avoid this, it is advisable for employees to either not state that they work for the school or to be non-specific (e.g. by stating that you work in 'local government' instead). You should also ensure that you always include a disclaimer, e.g. 'Views expressed here are my own and not that of my employer'. This must be displayed clearly on your profile.

2.3 When using a personal account you should not use the school logo, school email address or any other form of school identification.

2.4 Use discretion at all times. Ask your line manager if you are unsure as to whether your content may compromise the school in any way.

2.5 Through social media you are potentially connected to other school staff, councillors and residents, as well as the rest of the world. Make sure the image you project is consistent with your position in the school.

2.6 You need to ensure you are aware of your obligations to other school policies such as data protection i.e don't reveal or discuss confidential information or anything that could be damaging to the school or children.

2.7 The council has an agreed media protocol in place. Just as if officers were contacted by the media via email or over the phone, and requested to give a statement, comment or interview on behalf of the school this must be raised with the headteacher and with the Corporate Communications and

Marketing team.

2.8 If you find yourself in any doubt, check with the headteacher, the Corporate Communications and Marketing team and/or ICT.

3. Using social media professionally on behalf of the school (during and outside of working hours)

3.1 If managed properly, social media can provide a highly effective opportunity for the school to engage in conversations, share information and promote its services on a local, national and global scale.

3.2 In line with the communications, ICT and customer service strategies the school encourages two-way conversation with others, including citizens, partners, organisations, businesses and other parties, where relevant and appropriate.

3.3 If managed appropriately, the council supports the use of social media to highlight and promote the work of service areas. In the first instance this should be done through the approved channels which are managed by the Headteacher.

4. Guidance for employees using social media on behalf of the school (once your business case has been approved by the head)

4.1 Ensure you receive appropriate training and that you are listed as an official authorised user with the Corporate Communications and Marketing team and ICT.

4.2 If you have been granted permission to use social media for work purposes, this cannot be used for personal reasons. The ICT department can and will check the use of social media as set out in the ICT Code of Practise.

4.3 Be careful when choosing to share information posted by other users including individuals and organisations. Be mindful of endorsing someone else's activity as it could contradict council policy.

4.4 As with normal business, employees should remain politically impartial when representing the school via social media. This would mean school accounts should not engage in political debate, follow individual political parties or politicians, endorse electioneering campaigns for specific parties etc. This is not applicable for officers who are also trade union representatives when acting in their capacity as a union representative.

4.5 Social media should not be used in isolation to other forms of communication and marketing. Instead it should form a part of your service area's communication plans.

4.6 Social media lends itself to a less formal communication style. Ensure you are clear, professional yet informal in your tone. Avoid being flippant or sarcastic. Similarly you need to ensure you do not start using 'text speak' or abbreviations such as 'lol'.

4.7 Conversations on social media should add value and fit with the council's aims and objectives. Adding value means:

- Helping you, your fellow employees, our citizens, our customers and partners perform well and solve problems;
- Enhancing the school's services, processes and policies;
- Creating a sense of community;
- Helping to promote the school's aims and values;
- Providing 'news you can use'.

4.8 The same codes apply to online activity as do in your day to day working life. Users must be aware

of, and abide by the ICT Code of Practise.

4.9 If you suspect that your social media account has been hacked, please report this to ICT for advice on how to manage this.

4.10 Laws such as libel, defamation, copyright and data protection all apply online. For the council's protection, as well as your own, it's imperative that you conduct your behaviour appropriately:

- If writing on internal/sensitive school matters, seek permission before making public;
- If you share content created by others, for example photographs or videos, always get written permission. If you don't know who created the media then you must not use it as it might be liable to copyright;
- It's vital that officers understand data protection and the importance of not revealing personal data. The definition of 'personal data' is a wide field, but in the main part consists of information that can lead to the identification of others – directly, or if linked with other information. You should never post information that could potentially identify others. If you were found guilty of breaching the data protection act you, and the council, could face a hefty fine.

4.11 Be aware that all information that you publish on the Internet is viewable to a global audience and has the potential to always be viewable/searchable online. Content on social media sites may also be subject to Freedom of Information requests.

4.12 Ensure you put sufficient measures in place in line with the school's Customer Service Charter to respond to queries in a timely and accurate manner. Remember even though you might only use social media during office hours other users will access and generate content 24 hours a day.

4.13 Exercise caution when using social media applications (such as widgets) as some require you to allow access to your account. These applications often have a disclaimer that states they can access your account and post on your behalf – this often manifests in auto-updates when using the applications and can often be misconstrued as advertising. It is advised you refrain from using these.

4.14 If you are adding content onto social media platforms on behalf of the council then you're encouraged to be clear about who you are, use your real name, and identify that you work for the council. However, be careful not to reveal too much information when building a relationship with fellow users, as this could put you at risk of identity theft. It might seem obvious, but never give out personal details.

4.15 Deal with offensive comments quickly and sensitively. If an offensive, threatening or libellous comment is posted then you have the right to remove it (if possible) or ask for it to be removed by the person who posted it, however do give an explanation as to why you have taken this action.

4.16 Do not ignore difficult queries; instead deal with these publically in a professional and transparent manner. The purpose of social media is to encourage two-way conversations, part of this will include responding to difficult queries. Remember people are entitled to their own views. You may encounter persistent complainants who use social media to highlight what they feel is a personal issue or injustice. Always speak with your line manager or the Corporate Communications and Marketing team before responding. Sometimes a response is not always required. As a general rule:

- Make the effort to respond publically to the query so other users can see you are willing to help/solve the problem;
- If you are unable to answer the query utilise a holding response such as 'Sorry to hear this. We will find out some more information and get back to you asap.' Or 'Thanks for letting us know. We will get back to you shortly';
- Make sure you follow up on your promises and get back to people. If the situation doesn't improve please speak with your line manager or the Corporate Communications and Marketing team for further advice;

- There might be occasions when you may not be able to respond to a query via social media e.g. Twitter has limited character spacing. In these instances it is appropriate to say something along the lines of 'Sorry to hear this. This requires a response too detailed for here. Please message us your contact details so we can get back to you';
- The council has an agreed media protocol in place. If you are asked by the media to give a statement, comment or interview on behalf of the council this must be raised with your manager and with the Corporate Communications and Marketing team.
- Always be courteous in everything you write in any social media forum;
- If someone is not asking you a question, consider whether a response is actually required;
- If someone contacts you in Welsh in line with the council's Welsh Language Scheme and Customer Service Charter you need to ensure you respond to that person through the medium of Welsh using the council's approved translators.

4.17 Social media presents a great opportunity for us to develop close relationships with the public; however it is always an addition to your current role. You must manage it carefully so it doesn't impact on the requirements of your daily work. Please remember that internet activity is logged and can be monitored.

4.18 It is not enough to simply set up an account as it will not manage itself. People will expect two way communications and you need to be prepared for that. You need to pro-actively ensure the account is monitored regularly and that you are generating timely content otherwise it becomes a meaningless channel of communication and your followers will recognise and react to this. For tips on how to grow and develop your social media presence please contact the Corporate Communications and Marketing team.

4.19 Before posting content, make sure that it's factual, correct, timely and honest. If you post something in error and choose to delete it, consider whether you may need to clarify this and why you've done so. Remember, you ultimately have responsibility over what you've published so make sure you get it right. If you have any concerns then speak with the headteacher or the Corporate Communications and Marketing team.

4.20 You may come across inaccurate or incorrect content other people have generated about the school or your service area. Don't be defensive in reacting to this. If information is inaccurate or incorrect you may politely and sensitively clarify the situation. You must however inform the Corporate Communications and Marketing team of information posted that could damage the reputation of the council.

4.21 If in doubt with any points check with the headteacher or the Corporate Communications and Marketing team.

5. Sanctions

5.1 Where it is believed that an employee has failed to comply with this protocol action, the matter may be referred for consideration under the school's Disciplinary Policy.

6. Agreement

6.1 All school employees, contractors and agency workers who have been granted the right to use the school's internet access are required to accept this protocol.