

Birdlip Primary School

'Helping each other prepare for a bigger world'

Technology and E-Safety Policy
Written by: Mr. J Pugh, Apr 2024
Updated: April 2025
Review: April 2027

The purpose of this policy statement

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Birdlip's activities.

Contents of this policy

1. E-Safety
2. Acceptable Use - Staff
3. Acceptable Use - Children
4. Social Media and photographs
5. Online and blended learning
6. Use of tablets
7. The School Infrastructure
8. Appendices

---

1. E-Safety

E-safety is the school's ability to:

1. protect and educate pupils and staff in their use of technology
2. have the appropriate mechanisms to intervene and support any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content, for example: exposure to inappropriate content, including online pornography; ignoring age ratings in

games (exposure to violence, often associated with racist language); and substance abuse lifestyle websites, for example pro-anorexia, self-harm or suicide sites hate sites
- **Contact**: being subjected to harmful online interaction with other users; for example: grooming cyber-bullying in all forms of identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, privacy issues, including disclosure of personal information digital footprint and online reputation, health and well-being (amount of time spent online (internet or gaming)), sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) copyright (little care or consideration for intellectual property and ownership – such as music and film).

It is vital that e-safety is delivered by **all staff** in all environments, such as assemblies, newsletters and parent meetings, and in all areas of the curriculum. Although the school has an Internet filter and thus a managed system it is vital to teach children Internet safety as if the filter did not exist to ensure safe Internet use is adopted out of the school environment.

This policy in its entirety has been developed with staff, governors, parents and pupils. **Pupil voice** is used to gauge children's views, opinions and knowledge.

Staff training is paramount to ensuring the e-safety content delivered is relevant, up to date and accurate. A dedicated e-safety module is taught within our PSHE curriculum.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:
- online abuse
- bullying learning
- child protection

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using Birdlip's network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse

- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

Implementation:

- We have appointed an online safety coordinator and an e-safety governor to oversee this policy and monitor our e-safety provision.
- providing clear and specific directions to staff and volunteers on how to behave online through our acceptable use protocols (see §2).
- Implementing an e-safety scheme of work to be taught within PSHE and the wider curriculum.
- Providing and sharing regular information with parents to support and encourage parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that our domain, logins and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- Recording the incident in CPOMS, taking appropriate action and contacting the relevant bodies, such as parents or police.
- Ensuring every breach of e-safety serves as a learning experience for both pupils and adults.
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Key features of our practice

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e-safety issues. High quality leadership and management make e-safety a priority across all areas of the school. A high priority is given to training in e-safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems. Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. One or more members of staff have a higher level of expertise and clearly defined responsibilities.
Policies	Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors. The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The e-safety policy should incorporate an Acceptable Usage Policy that is understood and respected by pupils, staff and parents.
Education	An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-safety. Using data effectively to assess the impact of e-safety practice and how this informs strategy.

Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

---

2. Acceptable Use - Staff

Intent

The aim is to ensure that staff are aware about the acceptable use of technology both within the school setting and when using school information at home.

Implementation

Note: All Internet and email activity is subject to monitoring

Internet access – The Internet at school is filtered. You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting gender, racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and recorded on CPOMS.

Streaming – Live streaming is only allowed in the context of Remote Learning.

Social networking – is allowed in school in accordance with this e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should think very carefully about making "friends" with parents and never pupils on personal social networks. Please see Social Media, §3.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act. All school information which contains any data regarding children will only be sent to school email addresses.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that you work within the Birdlip domain and laptops should be securely password protected. Pen drives are discouraged and should only be used if they are password protected.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use

unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Viruses and other malware - any virus outbreaks are to be reported.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with children.

Laptop Computers - All staff have access to a laptop computer for school use. These are for school use, should be password protected and care must be taken to ensure no data is left on the screens when not in use.

Mobile Phones – Staff are allowed to carry and mobile phone in school. Phones should not be used for communication or social media throughout the working day unless on school business or during a break. No pupil data or photographs are permitted on staff mobile phones. Children are not permitted to bring mobile phones onto school premises unless with permission from the headteacher.

Tablets – All staff have access to a tablet device which can be used for Padlets, Doodle, or any other specific task. These can also be used to take and save photos to the staff Google Drive. These are always secured with a passcode.

GDPR - Staff have all been trained concerning GDPR protocols and are knowledgeable about keeping data safe and secure.

Online teaching and learning – There is an expectation to teach remotely when the school cannot be open (Please see Online Learning §5). We use a combination of Google Classroom and G-Suite Apps, specific websites and APPS (such as Spelling Frame and Doodle APPS) and live streaming (using Google MEET). Staff should be aware of every web link they direct children to and ensure parents are aware of what their children are doing. Any concerns about children's welfare or Internet safety should be reported to the headteacher.

Teaching on-line safety – From September 2020, RSHE is mandatory in primary schools. Through this, pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online action on others and knowing how to recognize and display respectful behaviour online. Through these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way and what is relevant to their pupils' lives. This will complement the computing curriculum – KSCIE 2021. (Please refer to Dfe Teaching Online Safety in School, June 2019)

Impact

Consistent safe use of technology by staff will ensure that online safety is role modelled to

children and that they remain safe at all times.

3. Acceptable Use Policy - Children

Our Charter of Good Online Behaviour

I Promise – to only use the school ICT for work that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use or share other people's work or pictures without permission to do so.

I will not – take pictures of anyone without their permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone and I let my teacher know if anybody asks me for personal information.

I will not – download or upload anything from or to the Internet unless my teacher has asked me to.

I will not – install or delete any apps on the school's iPads or Tablets.

I will not – bring in any electronic device from home (such as a phone or gaming device). If for any reason I need to for domestic reasons I will hand it to my class teacher at the beginning of the school day.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

4. Social Media

Intent

The internet and social media provide a range of social media tools that allow users to interact with one another.

It is recognised that there are benefits to effectively using social media for business and personal purposes. This policy provides clarity to the school community about the way in which social media is used and sets out expectations as to an employee's and other members of the community conduct regarding social media.

It is vital that pupils, parents and the public have confidence in the school's decisions and services and that the reputation of the school and the confidentiality of information about pupils and staff is safeguarded. We seek to ensure that school staff use social media responsibly and to avoid inadvertently placing themselves in a situation where their conduct is called into question due to unacceptable use of social media.

Scope

For the purposes of this policy, social media is any type of interactive online media that allows parties to participate in interactive discussions and share information in a public forum. It is important to note that this may apply to some forums that are private but are shared or made public i.e. the policy may extend to 'closed groups' where a matter in breach of this policy is brought to the attention of the school.

Examples of some popular forums are Twitter, Instagram, Snapchat, Facebook and LinkedIn, but social media also includes podcasts, open access online encyclopedias, social bookmarking sites, blogs and video, live streaming forums and image-sharing websites such as YouTube, Vimeo, and Instagram. It is impossible to list all relevant media as this is a constantly changing and growing area.

This policy applies to all paid employees of the school, teachers (including trainees and apprentices), volunteers and members of the Governing Body.

Employees of Gloucestershire County Council (GCC) are covered by Council's own social media policy and the school should report any suspected breach by a GCC employee to GCC.

Schools often use contractors to carry out work and may require contractors to have their own social media (acceptable use) policy in place.

This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained by and on behalf of the school.

For the purposes of this policy references and links to the County Council will not always apply to academies and other schools or settings that are independent from the local authority.

Legal framework

Employees must remember that information they share through social media and networks, even on private accounts, is still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006, and UK libel and defamation laws.

Both the School and the County Council could be held vicariously responsible for acts of their employees in the course of their employment (in local authority community and voluntary controlled schools). For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of any protected characteristic, or who defame a third party while at work may render the School or the County Council liable to the injured party.

Social media relating to the school

The School uses social media to promote and market the school. Use of pupil images are used with explicit permission from parents.

Authorisation to share specific school business via communication channels which cannot be directly managed by the school (such as personal social media) must be sought from the head teacher/Governing Body of the School prior to sharing.

This includes opinions shared on social media that can be, or perceived to be, attributable to the school, its representatives and/or its decision-makers.

Sharing of any aspects of school business or relevant communications from the school via authorised social media platforms used and managed by the school must be approved by the head teacher.

Any authorised messages must be constructed to be unambiguous, accurate, politically neutral, fair and transparent if they are to formally represent the School or the County Council.

Creation of social media accounts by school staff for use in education

All social media services must be approved by the head teacher/Governing Body of the school in advance of any educational work being undertaken.

Personal use of social media by employees

It is accepted that employees and members of the school community will have their own social networking accounts. However, it is important that they protect their professional reputation, the reputation of the school and the privacy of colleagues, pupils and parents.

Employees are required to familiarise themselves with social network sites' privacy settings and are encouraged to make their settings 'private' in order to ensure that information is not automatically shared with a wider audience than intended e.g. on Facebook opting out of 'public' settings.

Employees must be aware that even with high privacy settings, their posts are never truly private as friends/connections could save or share these posts, so this policy may still apply even if the profile is private.

Employees must not conduct or portray themselves, or allow friends to portray them, in a manner which may:

- bring the school into disrepute;
- lead to valid parental/carer complaints;
- be deemed as derogatory towards the school and/or its employees;
- be deemed as derogatory towards pupils, parents/carers or governors;
- bring into question their appropriateness to work with children (including behaviour that is illegal);
- contravene current National Teacher Standards (or other relevant professional standards).

In addition to posts written by the employee, this can also include posts that the individual has shared, liked, retweeted etc. as well as tagged photographs where the content contravenes this policy.

Further to this staff should not:

- form online friendships or enter into communication with parents/carers as this could lead to professional relationships being compromised;
- form online friendships or enter into online communication with pupils as this could lead to professional relationships being compromised, and/or safeguarding allegations being raised;
- post pictures of or negative comments about their employment, school events (sharing information and posting pictures about school events should be done through the school's authorised social media site(s) or with advance authorisation from the head teacher/Governing Body).

It is recognised that employees may be known in the community in which they work and may have connections to parents/carers of pupils on social media (either relatives or close friends). Employees in this situation are responsible for their own social media and hold such connections at their own risk. Breaches under this policy in relation to this type of connection are managed in the same way.

Further guidance on the use of social media

School workers (paid staff and volunteers) must be conscious at all times of the need to keep personal and professional lives separate on social media. School representatives should not:

- Put themselves in a position where there is an actual or perceived conflict between work for the school or County Council and their own personal interests.
- Engage in activities involving social media which might risk bringing the School or the County Council into disrepute.
- Represent personal views as those of the School or the County Council on any social medium.
- Discuss personal information about pupils, School business or County Council staff and other professionals interacted with as part of their role in the school.

Use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, carers, colleagues, other professionals, other Use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, carers, colleagues, other professionals, other organisations (e.g. OFSTED), the School, other schools or the County Council.

Unilaterally use social media as a communication channel about school business, even if that communication relates to matters which are already cleared to be shared with parents (Communication to parents is managed through the channels that have been approved by the Governing Body.)

It is recognised that personal use of social media can relate to professional life i.e. LinkedIn. However, employees identifying their place of work do so at their own risk and if this policy is breached in relation to those sites it is applied in the same way.

Breaches of the policy

Any breach of this policy may lead to disciplinary action being taken against the staff member(s) involved in line with the School's disciplinary procedure.

Inappropriate use of social media by employees or volunteers should be referred to the head teacher/Board of Governors in the first instance so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school and the County Council. In local authority community and voluntary controlled schools where there has been a breach of confidential information the breach must be reported to the Data Management team at Gloucestershire County Council.

A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the School or the County Council or any illegal acts or acts that render the School or the County Council liable to third parties may result in disciplinary action and dismissal from service.

Any illegal acts may be reported to the police and/or the relevant professional body.

Parents/carers (the 'wider' school community) on social media sites

Parents/carers will be communicated with regarding their use of social media (in particular when they or a child they are responsible for joins the school) via the school website, letter and school newsletters particularly with regard to the following:

- Parents/carers are asked not to post images (photos and videos) of pupils other than their own children participating in school events on social media sites unless they have the permission of parents/carers of other children pictured.
- Parents/carers are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media.
- Parents/carers should not post malicious or fictitious comments on social media sites about any member of the school community.

While the school cannot monitor all use of social media in the wider school community the communication to parents/carer aims to protect pupils and staff at the school and the confidentiality of information about pupils and staff.

Parents may take pictures and video clips of school plays and events but are requested not to post these on-line on any social media platform.

Dealing with incidents of online (cyber) bullying

Cases of online bullying will be dealt with in accordance with the school's fairness, diversity and equality and/or dignity and respect at work policies and could lead to action being taken under the disciplinary procedure.

The school can take action with reference to any incident that takes place outside school hours if it:

- could have repercussions for the orderly running of the school,
- poses a threat to a member of the school community,
- could adversely affect the reputation of the school, or its employees/governors.

There are UK statutes that cover the use of Internet technology in relation to bullying.

Where cyber bullying involves pupils it may be necessary to deal with this under a separate policy (e.g. the schools' Anti-Bullying policy).

Where appropriate, legal action may be taken by the school's governors.

---

5. Blended and On-Line Learning

Preamble
From October 2020, it became a legal requirement to provide education "virtually" if children or staff cannot attend school. There is a level of accountability placed on both class teachers and

teaching assistants to ensure pupils are "schooled" and make progress which will be monitored by the school.

Blended Learning – Children learning at home when they are unwell, isolating or during school closure. Children are occasionally at home but are well enough to study.

On-Line Learning – When a whole class is required to learn remotely from home or the class teacher is at home and needs to teach the class remotely.

Resources

All the children have a Google account within the Birdlip.org domain. Mr Pugh has admin control which includes resetting passwords and downloading APPS.

- Google Meet – video
- Google Classroom – comprehensive package from on-line notice board to instrument to set, mark and return work
- Google Docs, Slides and Sheets and Forms – Office applications
- Google Drive – Storage place for all children's work
- Jamboard – online live whiteboard
- Spelling Frame

This list is by no means exhausted.

Staff Expectation
Class teachers are accountable for pupils' learning and are thus expected to set, teach and assess work in order for pupils to progress. Teaching Assistants are expected to assist teachers, working their individual working hours. Staff are expected to be available on Google Meet during school hours (9.00-12.30 and 13.30 to 15.00) and demonstrate time spent teaching rather than merely providing activities.

Pupil Expectation
Pupils are expected to engage with our on-line provision. Ospreys all have a tablet and there are a further 30 tablets which can be lent out. There is no expectation that children always work "live" but can complete tasks later in the day. The school also uses Doodle APPS and SpellingFrame to supplement learning. A register will be kept to monitor attendance and work submitted. There will be a vast difference between the method of operandi for KS1 and KS2 due to their learning process and age difference. There is no legal grounding to "force" children to learn remotely but the realisation it is in the child's best interest.

Activity Expectation
The activities should loosely follow the curriculum plans although not all activities will be taught. There should be a range of mathematical and Literacy work combined with creative and exploratory activities. Work can be done on Google Classroom, Paper and orally.

Safeguarding

Reference: Safeguarding and Remote Education, Keeping Children Safe in Education, Annex C, School's Safeguarding policy

Keeping pupils, students and teachers safe during remote education is essential. Teachers delivering remote education online should be aware that the same principles set out in the school or college staff behaviour policy (sometimes known as a code of conduct) will apply.

Below are resources to understand more about how to ensure online education is safe:

- advice from NSPCC on undertaking remote education safely
- guidance from the UK Safer Internet Centre on remote education
- Kirklees College developed and disseminated a safeguarding protocol specific to the context of remote learning
- Digital Wellbeing of Learners guide from Jisc which curates a number of resources and guides
- National Cyber Security Centre (NCSC) guidance on how to work from home - supporting college staff to ensure Prevent and security policies are maintained from home

Reporting Concerns: In accordance with the school's safeguarding policy all concerns should be reported adhering to school procedure.

Activities

Activities will be set through Google Classroom each day. Work will be submitted in a variety of ways, such as using Google Forms or posting photos on Google Classroom. We will continue to make use of the Doodle apps and Spelling Frame. TA support will be available daily in small groups or on a one-to-one basis.

Class Specific Methodology for blended learning activities

On the occasion that a minority of children are at home, the class teacher will provide activities and/or a live lesson through Google Meet to run alongside the school activities. Whilst the priority will be the children at school, every effort will be made to supply activities and provide teaching. **Children who are unwell are not expected to participate.**

6. Use of Tablets

Intent
Children in Ospreys have access to a tablet device to be used for school work using Google Classroom. It is expected that these devices will be used at home and school to extend learning and promote independent work.

Safety first
- At school all on-line searches and websites are strictly filtered by RM. Each device will need to be configured to join the schools' Wi-Fi.
- At home, it is highly recommended that parents install a filter and it is suggested that parents devise rules regarding time and place where these tablets are used.
- All work on Google Classroom and using the G-Suite apps will be operated within the Birdlip domain. There is no scope to send work in and out of the domain.
- Devices are individual and should not be shared, all tablets should be locked with a passcode (please let Mr Pugh know what it is!).
- All videos that are put on YouTube are strictly monitored and will always be unlisted. (only staff members are able to upload onto YouTube).
- The school reserves the right to monitor Internet search history on devices used at home
- All parents / carers need to sign an agreement to honour our e-safety policy and adhere to safe use of tablets and Internet use at home.

Tablets
The school will keep a record of serial numbers of all tablets. However, it is the children in Ospreys' responsibility to bring them to school each day, keep them
safe, look after them, ensure they are charged and manage them with regard to files and photos.

Passwords
Passwords are very important and should be kept secret. Do not tell your friends and ideally, they should contain upper and lower case, numbers and symbols. Mr Pugh can reset passwords to school apps and accounts.

Social Media
Social media such as Instagram, Facebook, Twitter, Tik Tok, Snap Chat, etc are age specific and are not to be used by Birdlip children.

Insurance
Tablets should be covered by home insurance. In the event of accidental damage, the school is prepared to help, if appropriate, up to a maximum of £100. In the event of malicious damage compensation will be sought from perpetrators.

Charging
Children should take responsibility in ensuring that tablets are charged ready to be used each day. There are charging posts in the classroom for emergencies.

Google Accounts

On each device provided by the school, there should be a minimum of 2 google accounts:

1. Device@Birdlip.org. This is the admin account which will deliver apps and the Internet certificate.
2. username@Birdlip.org. This is a pupil's individual account with space for photos and files. All work is done within the Birdlip.org domain. Apps cannot be downloaded.

If you would like to extend learning at home with a tablet, we recommend installing the following APPS. They are all free:

Google Drive	Google Sheets	Google Keep
Google Classroom	Google Docs	G mail
Google Meet	Google Slides	Doodle Maths
Google Hangouts	Google Calendar	Amazon Kindle
Google Jamboard	Google Chrome	Duolingo

---

7. The School Infrastructure

The School has a simplistic model.

- The Internet is provided by RM. Plan to move to Gigaclear
- A managed switch allow the internet to be passed through Ethernet points and WiFi access points
- Some laptops are used and operate within a network. Plan to remove the network and move to the cloud.
- Printers are on the network. Plan to ensure all tablets can print
- RM is used as an Internet filter and as a system to monitor individual devices. Plan to change to a DNS filter
- Each member of staff has access to a school laptop
- All staff also have access to a tablet
- 4 classrooms have a large screen to show work
- All children in Ospreys have use of their own Lenovo tablet
- All children in Golden Eagles and Kingfishers have access to a Lenovo tablet
- Children in Robins have access to iPads
- All children, staff and governors have a Google account within the Birdlip.org domain
- The Birdlip domain is secure and managed by Google Admin. This has been professionally checked.
- The school uses Google Classroom as a means to distribute work, share information and as a platform for online learning
- Other APPS are used, for example Doodle, G-Suite
- All Google passwords are managed by Mr Pugh.

8. Appendix

Glossary of terms

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection and Safeguarding Policy 2021
- Safeguarding and remote education during coronavirus
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures

Responsibilities

E-Safety: Mr Pugh
Computing Subject Lead: Mr Pugh
E-Safety Governor: Mr A Ghosh