Online Learning Policy

In God's love, aspire and achieve to be the best'
1 Corinthians 16:14 'Do everything in love.'

The impact of Covid-19 and the closing of schools for a period of time ensured that we all had to adapt to new ways of working.

Remote learning ensures that valuable education is not lost through exceptional circumstances and should be valued by the school and parents.

This policy is not meant for when children are not well or because of a term time holiday.

Single child

If your child is well but unable to attend school, the work that they are missing in school will be posted on Google Classroom for them to complete. If possible the class teacher or teaching assistant will contact home to explain what to do. Work should be submitted on Google Classroom for the teacher to give feedback. If the period of home learning is more than a few days the class teacher will phone home to speak to the child and parents at least once a week.

For children who do not have a device or internet access

For those who are entitled to free school meals, the school will loan a school device. If the family does not have internet access then paper copies of work will be provided.

Expectations of teachers(unless unwell)

If the whole class has to be away from school, teachers will;
- provide appropriate work for children during times they are unable to attend school. There will be a minimum of one piece of Maths and English each day, plus at least one other subject. The work will be posted on Google Classroom.
- be mindful that some children may not have an adult at home that is available to support them with their learning and so will also provide work that the child should be able to access independently. It is recognised that this is much more difficult with younger children.
- Keep a register of engagement from children.
- monitor Google Classroom throughout the usual school day to answer any questions.
- mark all work submitted within a given time frame.
- provide daily contact to explain the learning for the day through. For those that do not have internet access, this will be done via telephone.
- monitor SEND children.
- contact parents if there is no work submitted to see if there are any problems.
- If the teacher is unwell, the teaching assistant will monitor the Google Classroom and support the marking of work. If a teacher is ill and cannot record/upload work then children will be directed to the Oak Academy for their lessons.
- Report any safeguarding concerns to the DSL.
- Ensure confidentiality and integrity of electronic devices whilst working remotely.

Expectations of parents

We appreciate that supporting your child at home can be very challenging, especially if you have to work yourself or have very young children. However, we hope that parents will;

- provide their child with a device to use to access the remote learning. They should contact school if they cannot provide a device.
- support their child whenever they can to access the learning provided.
- ensure that a minimum amount of work is done each day (please see individual class expectations).
- let the school know if there are any problems accessing the learning.
- request paper copies of work if you do not have internet access.
- Support your child to access work safely such as adding parental controls and anti-virus software.

Expectations of children
- KS2 children should be able to take some responsibility for their own learning.
- KS2 children will be shown how to access the learning on Google Classroom and how to submit work.
- Children should agree to do some school work every day during any isolation period as they would at school.
- Complete paper copies of work if they do not have access to a device or internet.
- Complete their work to the same standard they would if they were at school.
- Report any safeguarding concerns.

The headteacher will;
- Monitor the quality of work provided by class teachers.
- Monitor the register of learning engagement.
- Provide information to parents about school updates.
- Deal with any safeguarding concerns raised and ensure that vulnerable pupils are monitored for online safety.
- Ensure that any loaned equipment is safe and does not breach any data protection rights.
- Make regular contact with vulnerable pupils.
- Evaluate and manage risks associated with remote learning.

The SENCO will:
- Ensure that children with an EHCP have their needs met whilst learning remotely.
- Ensure that provision is made for children with SEND and that the provision is monitored for effectiveness.
- Contact families that may require additional support.

Google Classroom in GSuite for Education

Safeguarding

The following steps have been taken to ensure that staff and students stay safe when using google classroom.

November 2020

- Google classroom was set up by our own tech support company (EDAC) to ensure all safety features were installed.
- Only certified members of the school community (who have a school email) can join the google classroom.
- Children cannot send emails to anybody outside of the network.
- Children cannot organise video conferences using google hangouts.
- Following on from initial Warrington Borough Council Guidance we will not be holding live video conferences with the children – if a point in time arises where we need to do this we will follow the risk assessment attached to this document.

We use G Suite for Education - a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. Pupils will use their G Suite accounts to complete assignments, communicate with their teachers and learn 21st century digital citizenship skills, using mostly Google Classroom.

We use a special version of the core G Suite Apps to provide a secure learning intranet for our pupils and staff.

Children use a Gmail login to access our system servers and the intranet and internet in school. With school Gmail and Google Docs, for example, work and emails cannot be shared with external email accounts, only with others within @winwickprimary - the school's Google domain. Google require basic information to set up these accounts, a child's leaving year and name.

Google Cloud does contain much of the electronic work that your child completes in school. By logging in at home, using the same login as at school, your child can continue working on projects started in school, often using one of the main apps of G Suite, Google Classroom.

Our pupil accounts have a particular set of security settings to reflect the fact that the system is being used by a child - they have a much higher security setting than our staff for example. We take advice on these settings from EDAC

On leaving the school, we can transfer your child's digital learning record to his/her own gmail account through the Google TakeOut system - the school does not then retain any data. This can be a wonderful souvenir of learning. Google accounts will be deleted within weeks of leaving Winwick CE Primary.

Google's Privacy Policy for GSuite can be found here:
https://policies.google.com/privacy/update

The information below from Google provides answers to common questions about what they can and can't do with your child's personal information, including:

November 2020

What personal information does Google collect?
How does Google use this information?
Will Google disclose my child's personal information?
Does Google use student personal information for users in K-12 schools to target advertising?
Can my child share information with others using the G Suite for Education account?

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from pupils in connection with these accounts.

Using their G Suite for Education accounts, pupils may access and use the following "Core Services" offered by Google Classroom (described at https://gsuite.google.com/terms/user_features.html):

Gmail
Calendar
Docs
Sheets
Slides
Forms
Drive
Sites

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html

This information can be viewed in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a pupil account, we provide Google with certain personal information about our pupils, including, for example, a name, email address, and password. Google may also collect a profile photo added to the G Suite for Education account, but the school will not support the upload of personal photos of children.

When a pupil uses Google services, Google also collects information based on the use of those services. This includes:

device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;

log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address; location information, as determined by various technologies including IP address, GPS, and other sensors; unique application numbers, such as application version number; and cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

Does Google use student personal information for users in primary schools to target advertising?

No. For G Suite for Education users in primary and secondary schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can a child share information with others using the G Suite for Education account?
We allow pupils to access Google services such as Google Docs and Sites, which include features where users can share information with others within our Internet domain here at Winwick CE Primary.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organisations and individuals outside of Google unless one of the following circumstances applies:

With parental or guardian consent. Google will share personal information with companies, organisations or individuals outside of Google when it has parents' consent which may be obtained through G Suite for Education schools. We would contact parents directly if Google ask for any examples of children's work etc.

With Winwick's School G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.

For legal reasons. Google will share personal information with companies, organisations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

meet any applicable law, regulation, legal process or enforceable governmental request.

enforce applicable Terms of Service, including investigation of potential violations.

detect, prevent, or otherwise address fraud, security or technical issues.

protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices does a parent or guardian have?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting Mr Henaghen.

If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit https://myaccount.google.com while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, please contact Mr Henaghen.

If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the G Suite for Education Privacy Center, the G Suite for Education Privacy Notice, and the Google Privacy Policy.

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement.

Children have been made aware of online behaviour, however it is relevant that you are also aware.

Pupils need to know:

Pupils will follow school policies for appropriate use when using Internet based services like Web 2.0 applications & Google Apps. These services are considered an extension of the school's network.

November 2020

Pupils have no expectation of privacy in their use as school and service administrators have the right and ability to monitor user accounts for policy and security enforcement, whether they access these in school or at home.

Parents need to know:

Pupils email is archived and the Pupil Acceptable Use Agreement (PAUA) will be enforced. School staff will monitor pupil use of applications when students are at school. Parents are responsible for monitoring their child's use of applications when accessing programs from home; the school cannot take responsibility for home Internet access and its setup. Pupils are responsible for their own behaviour at all times.

Appendix A

E-Safety Online Video Conferencing Risk Assessment:

If you want to use live video conferencing with your students, you should set out some agreed 'rules' first. Suggested communication method of the below risk assessment points are via Google
Classroom prior to your online session:
● Any group chats should happen using only college email addresses and official college accounts (Microsoft or Google)
● If you think there is anything inappropriate then you should follow normal safeguarding procedures in report in the usual way via senior tutors and CPOMS.
● Students should turn off their video camera before joining the conference (they can see you but you won't be able to see them)
● Students should be respectful of other users in the language that they use and in their onscreen behaviour (ie not take control of the screen!)
● Students must use an appropriate space in the house where practical.
● You should warn them before you start that you will record the interaction
● Online meetings should happen within normal college hours i.e. 9.00 until 4.00 where possible/practical and on weekdays during term time
● If students are unable to use your microphone or have specific questions, then please use the text chat function in order to interact.

Appendix B –

Warrington Borough Council

WARRINGTON
Borough Council

November 2020

Guidance for using video conferencing

1. Introduction
Warrington Borough Council are responsible for managing the information we hold about service users and our citizens. We take our responsibilities seriously and use personal information fairly, correctly and safely in line with the legal requirements set out by the General Data Protection Regulation (GDPR) and other appropriate data protection legislation. This document sets out the expectations for Council employees using video conferencing and to use these in a manner that ensures our compliance with GDPR and the Data Protection Act 2018.

2. What do we mean by video conferencing?
"Video Conferencing" here refers to such applications but is not limited to those below-
☐ Skype for Business
☐ Skype
☐ Cisco WebEx
☐ WhatsApp
☐ Google Duo

3. How do I stay compliant when using video conferencing?
☐ Only use Council approved Video Conferencing software/applications to carry out Video Calls for work. These have been checked to ensure they provide you with a secure and safe connection for your call.
☐ Only use a Council provided device to make these calls. Our devices are configured securely to protect you and those you are calling.
☐ Where possible only make video calls whilst on the Councils network or on a network you can trust. Not, for example, an unsecured Wi-Fi network in a hotel.
☐ Always install available security patches and updates for your Council device and video conferencing software.
☐ Be careful with whom you share the details for your video conference - if the function to password protect the meeting is available, use it to protect against people snooping on your meeting.
☐ When talking to customers or colleagues over the phone always ensure that your conversation cannot be overheard.
☐ Don't let any friends or family members see or overhear video calls especially if you are working from home
☐ Be aware of any smart devices which use voice recognition such as Siri or Alexa as making a call near these could result in the audio being recorded and stored, without knowledge or agreement.
☐ Conference calls or video conferences should not be recorded. Any recordings either audio, video or both would need to be provided by yourself in the event of a subject access request.
☐ A data protection impact assessment (DPIA) should be completed for any new use of these technologies for the sharing or discussion of personal data. The Information Governance Team can provide guidance on this.
☐ Screenshots should not be taken during the conference call or video conference. Any

screenshots would need to be provided by yourself in the event of a subject access request.
☐ If you have to share your screen, be careful with what is displayed as you may have on the screen sensitive information or emails which you would not want others to see. Where possible share a single screen or a single application.
☐ Do not allow meeting attendees to control your desktop without your permission, and ensure that when the meeting is finished that the sharing and meeting is closed.
☐ Be mindful of your audience and ensure the meeting content is tailored appropriately to it. For example if you have external parties also attending the meeting, do not assume that any information presented or shared via the meeting will remain confidential. Unless there is a nondisclosure agreement in place, understand that there is a risk to the information being uncontrolled and shared on or used without our consent.
☐ If you have to leave a voicemail or use the 'Leave a message' function, please ensure that the message contains minimal personal data. For example your name and phone number would be considered necessary, but asking about or referring to any physical or mental health conditions during this would not be acceptable under the Data Protection Act.
☐ Do not use the meeting software to share files. While it might be easy to do so, files should not be sent via this method and if there is a need to share, standard Council methods for file transfer should be adhered to in order to protect the data and to provide an audit trail.

4. Further Information & Support
☐ For information on completing a DPIA please contact the Information Governance team via informationgovernance@warrington.gov.uk
☐ For information on data protection and information governance please see https://intranet.wla.int/RASC/BIS/_layouts/15/start.aspx#/SitePages/Information%20Governance%20And%20Corporate%20Records%20Management.aspx