CUNDALL MANOR SCHOOL

11.1 ICT Acceptable Use Policy

The development of new technologies has become integral to the lives of children in today's society, where the internet, digital information and communication tools can stimulate discussion and promote creativity.

This policy is intended to ensure that:

- **children and adults will be responsible users and stay safe while using the internet, other communication technologies and digital resources for educational, personal and recreational use,**
- **school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.**

This policy covers pupils and staff. Staff should familiarise themselves with the complete document.

Cundall Manor School (CMS) will try to ensure that pupils and staff have good access to ICT to enhance their teaching and learning and will expect the pupils and staff to agree to be responsible users in return.

Parent will be asked consent to the Acceptable Use Policy on joining the school and again at the beginning of each academic year having read through it with their children.

All staff will sign the ICT Code of Practice for Teachers and Adults on joining the school and again at the beginning of each academic year.

CMS uses the Sophos web filtering software. Sophos web filtering uses a true real-time web content filter; it performs live analysis and real-time categorisation of web pages to dramatically improve protection and security. In a remote learning setting parents must take responsibility for monitoring their child's internet use as the school cannot regulate this activity off site.

Pupils' use of internet

- Use of the internet, including e-mail, is permitted as directed by the teacher for purposes of research and learning directly related to the curriculum.
- Pupils will not be permitted to introduce or download executable files (e.g. '.exe, .cmd, .bat, .bin') to the network as these can in some cases contain harmful viruses. This includes but is not limited to copying such files onto the PupilShared (M) drive, saving them to your Home Directory (Z) drive or Google drive and running them from a USB Memory Stick.
- Pupils will not be permitted to introduce or download music and video files (e.g. '.mp3, .mp4, .mpeg, .wav, .avi'). These files in many cases are copyrighted and the copying onto the school network or the workstation may breach their copyright.
- The use of game-style activities should be monitored by the member of staff to determine suitability. Games which are not age appropriate contain violence, inappropriate language or behaviour demeaning to others are **not** permitted. Pupils are to follow any directions relating to gaming activity from the supervising member of staff.
- Accessing websites that contain content and images which are not age appropriate, ie. from a film, television programme or game deemed to be for older viewers, is not permitted.
- Images from the Internet are not to be accessed, downloaded or printed without prior permission from the supervising member of staff.
- Pupils are permitted to view online videos. They are to follow any directions relating to online video activity from the supervising member of staff.
- Non-school e-mail, social networking or instant messaging sites are **not** permitted during school times. They will only be available during the week between 5pm and 10pm and weekends between 9am and 6pm.
- Children should report any misuse of the internet to their teacher.
- Pupils must not access websites that incite radicalisation or compromise the fundamental British values held by the school.
- Children should be made aware of the possibility of online bullying and the increasing threat of radicalisation via the Internet.
- When using email pupils of CMS should always remember that they are representing themselves and our school and that all emails are logged by the school in case any concerns are raised. No CMS email should include information that may offend; or fail to respect the rights, beliefs and feelings of others.
- Personal information such as full names, home addresses, and phone numbers should **never** be sent by e-mail.
- We reserve the right to investigate incidents that take place outside school hours, on school visits and trips and that occur in the vicinity of the school, involving our pupils

Pupil use of the school network

- All pupils will be given a user name to access the network. Pupils must log onto the school network using their personal user name only.
- Pupils must not work at or tamper with a station that has been logged on by another user, even for short periods of time.
- Pupils must only access information stored on the shared area pupilshared (M) drive or your personal Home Directory (Z) or Google drive.
- Pupils must not edit or delete any information that is stored on the Shared Area.
- Pupils will ensure they log off after they have finished their session and leave the workstation in a tidy manner.
- Pupils will not use the network in any way that would disrupt the use of the network by others.
- Pupils will not introduce “USB drives” or other portable devices into the network without having them approved and checked for viruses by the ICT Manager.
- Pupils must not reveal their passwords to anyone, if they think that someone is using their logon details they must inform a teacher or contact the ICT Manager.

Acceptable use agreement – Junior and PrePrep (Reception to Form 4)

Dear Parents / Carers,

The internet is an amazing resource for us in school. It enables children to gain access to an unprecedented level of information. ICT allows your child access to a variety of interactive learning resources which stimulates both learning and creativity.

Unfortunately, the use of the internet is not without its dangers and some materials accessible through it are inappropriate for children. However, whereas no system can be guaranteed to be 100% safe, the huge benefits far outweigh the disadvantages and, at school, we use every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems.

Whilst the school monitors ICT use in school it needs to be understood that children also have an important responsibility themselves as to how they use the internet and school equipment. In a remote learning setting parents must take responsibility for monitoring their child's internet use as the school cannot regulate this activity off site.

Please read through this ICT Pupil Acceptable Use Policy with your child, discuss the points and impress upon them how important these are. You know your child and how much detail you will need to go into on the specifics.

Cundall Manor School

Pupil Acceptable Use Policy (Reception – Form 4)

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These 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 and are in essential in times when remote learning is required. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure*:*

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school systems (including Google or other accounts set up by the school) in a responsible way used at school or remotely, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

Computer Rules	
	I will only use polite language when using computers.
	I must not write anything that might upset someone or give the school a bad name.
	I know that a member of staff will regularly check what I have been doing using school computers or online school accounts.
	I must not tell anyone my name, where I live, or my telephone number over the Internet.
	I must not tell my username and passwords to anyone else but my parents.
	I must never use other people's usernames and passwords or computers left logged on by them.
	I must log off after I have finished with my computer.
	I know that any electronic message is not guaranteed to be private and could be forwarded without my knowledge.
	I will report any websites that make me feel uncomfortable to a trusted adult.
	I will tell my parents or a teacher straight away if I am sent any messages that make me feel uncomfortable.
	I will not try to harm any equipment or the work of another person on a computer.
	I will not attempt to download material that is not suitable for my age.

Behaviour Policy & Code of Conduct for Remote Learning

All normal school rules apply when pupils are engaging in remote learning.

Key principles:

· Every pupil must behave online with the same expectations of behaviour when behaving face-to-face with others; without exception, treat all others with respect.

· Google Classroom, Google Meet and all other GSuite applications including pupil mail accounts effectively operate within the School IT Systems and are monitored (as would be the case in any school or business).

· The sole purpose of Google Meet is to educate all pupils of the School remotely; no 'social' interaction must take place other than for educational and school community purposes

Google Meet (video conferencing) Etiquette

· All communication using Google Meet (or other video conferencing tool) must be of the same standard as expected in the classroom.

· Technology should be used in appropriate areas of the family house; if you use your bedroom as a workspace, then you should have your bedroom door open.

· Only teachers will initiate video conferencing.

· When using video, both pupils and staff must wear appropriate clothing.

· Any video conferencing or voice conferencing may be recorded by staff and stored securely in accordance with GDPR regulations.

· It is forbidden for any pupil to use a second device to record or photograph any material on Google Meet or any other live or recorded material of another pupil or teacher.

· Any material on Google Classroom, be it files, messages or videos must only be shared within the Cundall Manor School (CMS) pupil community for the purpose of learning.

It would be considered a serious disciplinary offence if any pupil was to tamper or interfere with systems in place to promote the learning for all on any of the platforms being used for remote learning. Any abuse directed at pupils or staff will be dealt with under the Behaviour and Sanctions Policy.

We all have an individual responsibility to ensure that remote learning is a positive experience for all.

GSuite For Education

At CMS we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is 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. At CMS, students will use their G Suite accounts to complete assignments, communicate with their teachers, sign into their Chromebooks, and learn 21st century digital citizenship skills. G Suite and Google Classroom provide a pathway for pupil teacher communication and a location to store set and returned work. When working from home, it is expected that our younger pupils will need parental support to log in and check for work or manage emails.

The appendix to this document provides answers to common questions about what Google can and can't do with your child's personal information, including:

- 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 schools to target advertising?
- Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions. Then fill out the online consent form using the link provided. If you do not provide your consent we will discontinue all G Suite activity relating to your child. Students who cannot use Google services will not have access to our remote curriculum.

For pupils in reception through to form 4 we have restricted email addresses to only allow them to communicate directly with staff, receiving and responding to work provided through Google Classroom.

Pupil User Agreement for the Pupil Acceptable Use Policy

Please now fill out the online acceptable use form (go here https://docs.google.com/forms/d/e/1FAIpQLSeKg8iXZ1nKphMdAV6m8NaecRTQW03bH5AW4dp06dwAg41nZA/viewform?usp=sf_link) to confirm the following statements.

I confirm that I have spoken to my child and they agree to follow the school rules when using the school computers and any accounts set up by the school. They will use the network in a sensible way and follow all the rules in the acceptable use policy. If they do not follow the rules, I understand that this may mean they might not be able to use the computers and/or Google account. I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the computers or accounts may have their use stopped, more closely monitored or past use investigated.

Appendix

G Suite for Education Notice to Parents and Guardians

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

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

- Gmail
- Google+
- Calendar
- Chrome Sync
- Classroom
- Cloud Search
- Contacts
- Docs, Sheets, Slides, Forms
- Drive
- Groups
- Hangouts, Hangouts Chat, Hangouts Meet, Google Talk
- Jamboard
- Keep
- Sites
- Vault

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 You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, CMS may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account, although this should not be needed.

When a student 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 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 my child share information with others using the G Suite for Education account?

CMS may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. Although most work will only be shared internally between teachers and their classes, from time to time classes will produce work that is shared publicly. When users share information publicly in this way, it may be picked up and displayed by search engines, such as Google and accessed by users all across the internet.

Will Google disclose my child's personal information?

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

- **With parental or guardian consent.** Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- **With** CMS**.** 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, organizations 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 do I have as a parent or guardian?

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 the IT Manager at CMS. 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 David Todd at davidtodd@cundallmanor.org.uk 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 (at https://www.google.com/edu/trust/), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html)

Acceptable use agreement – Senior (Form 5 to Thornton)

Dear Parents / Carers,

The internet is an amazing resource for us in school. It enables children to gain access to an unprecedented level of information. ICT allows your child access to a variety of interactive learning resources which stimulates both learning and creativity.

Unfortunately, the use of the internet is not without its dangers and some materials accessible through it are inappropriate for children. However, whereas no system can be guaranteed to be 100% safe, the huge benefits far outweigh the disadvantages and, at school, we use every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems.

Whilst the school monitors ICT use in school it needs to be understood that children also have an important responsibility themselves as to how they use the internet and school equipment. In a remote learning setting parents must take responsibility for monitoring their child's internet use as the school cannot regulate this activity off site.

Please read through this ICT Pupil Acceptable Use Agreement with your child, discuss the points and impress upon them how important these are. You know your child and how much detail you will need to go into on the specifics.

Cundall Manor School

Pupil Acceptable Use Agreement (Form 5 - Thornton)

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These 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 and are in essential in times when remote learning is required. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems (including Google or other accounts set up by the school) in a responsible way used at school or remotely, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

Computer Rules	
1	I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
4	I realise that files held on the school network and online accounts can be regularly checked by the IT Manager or other members of staff.
5	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network or internet.
6	I will work at my own computer and not deliberately interfere with the work or accounts of another pupil.
7	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
8	I will ensure that I log off after my network session has finished.
9	If I find an unattended machine logged on under another user's username I will not continue using the machine – I will log it off immediately.
10	I understand that I will not use social media or attempt to gain access to it while in school.
11	I am aware that an electronic message is not guaranteed to be private and that it can be forwarded without my knowledge. Messages that are supportive of illegal activities will be reported to the authorities. Anonymous / unnamed messages are not permitted.
12	I will not use the network in any way that would disrupt use of the network by others.
13	I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to a member of staff
14	I will scan any "USB drives" or other portable devices introduced to the network for viruses.
15	I will not attempt to visit websites or download material that might be considered inappropriate for my age or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
16	I will not attempt to download and/or install any unapproved software, system utilities or resources from the Internet.

17	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
18	I will not attempt to harm or destroy any equipment, work of another user on the school network, or on another website or account connected to the school system.
19	I will not bring a mobile phone into school or on any school trip unless specifically given permission by the member of staff in charge. If a phone is required before or after school it should be handed in to reception before the start of school and collected at the end of the day.
20	Additional electronic devices are not allowed on the school premises unless permission has been given by teachers or learning support staff. In which case, an additional acceptable use form will be required and all such devices should be inspected by the IT Manager before use in the school environment.

NETWORK SECURITY

If you discover a security problem, for example being able to access other user's data, you must inform the IT Manager immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

Behaviour Policy & Code of Conduct for Remote Learning

All normal school rules apply when pupils are engaging in remote learning.

Key principles:

· Every pupil must behave online with the same expectations of behaviour when behaving face-to-face with others; without exception, treat all others with respect.

· Google Classroom, Google Meet and all other GSuite applications including pupil mail accounts effectively operate within the School IT Systems and are monitored (as would be the case in any school or business).

· The sole purpose of Google Meet is to educate all pupils of the School remotely; no 'social' interaction must take place other than for educational and school community purposes

Google Meet (video conferencing) Etiquette

· All communication using Google Meet (or other video conferencing tool) must be of the same standard as expected in the classroom.

· Technology should be used in appropriate areas of the family house; if you use your bedroom as a workspace, then you should have your bedroom door open.

· Only teachers will initiate video conferencing.

· When using video, both pupils and staff must wear appropriate clothing.

· Any video conferencing or voice conferencing may be recorded by staff and stored securely in accordance with GDPR regulations.

· It is forbidden for any pupil to use a second device to record or photograph any material on Google Meet or any other live or recorded material of another pupil or teacher.

· Any material on Google Classroom, be it files, messages or videos must only be shared within the Cundall Manor School (CMS) pupil community for the purpose of learning.

It would be considered a serious disciplinary offence if any pupil was to tamper or interfere with systems in place to promote the learning for all on any of the platforms being used for remote learning. Any abuse directed at pupils or staff will be dealt with under the Behaviour and Sanctions Policy.

We all have an individual responsibility to ensure that remote learning is a positive experience for all.

GSuite For Education

At CMS we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is 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. At CMS, students will use their G Suite accounts to complete assignments, communicate with their teachers, sign into their Chromebooks, and learn 21st century digital citizenship skills.

The notice in the appendix to this document provides answers to common questions about what Google can and can't do with your child's personal information, including:

- 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 schools to target advertising?
- Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions. Then fill out the online consent form using the link provided. If you do not provide your consent we will discontinue all G Suite activity relating to your child. Students who cannot use Google services will not have access to our remote curriculum.

From form 5 email access is set so that pupils can contact and be contacted by addresses outside of the school system. They must still regard this email address as for school purposes exclusively, i.e. work collaboration with their peers, contacting their Spanish pen friends, or communicating with their parents. The address is not for arranging gatherings or signing up for social media or gaming accounts online.

CMS takes your child's welfare very seriously. As such, unlike a standard email system all emails will be scanned for language and logged at school so they can be checked through for appropriateness periodically. If any inappropriate use is detected pupils can be returned to staff only contact immediately.

Pupil User Agreement for the Pupil Acceptable Use Policy

Please now fill out the online acceptable use form (go here https://docs.google.com/forms/d/e/1FAIpQLSeKg8iXZ1nKphMdAV6m8NaecRTQWo3bH5AW4dp06dwAg41nZA/viewform?usp=sf_link) to confirm the following statements.

I confirm that I have spoken to my child and they agree to follow the school rules when using the school computers and any accounts set up by the school. They will use the network in a sensible way and follow all the rules in the acceptable use policy. If they do not follow the rules, I understand that this may mean they might not be able to use the computers and/or Google account. I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the computers or accounts may have their use stopped, more closely monitored or past use investigated.

Appendix

G Suite for Education Notice to Parents and Guardians

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

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

- Gmail
- Google+
- Calendar
- Chrome Sync
- Classroom
- Cloud Search
- Contacts
- Docs, Sheets, Slides, Forms
- Drive
- Groups
- Hangouts, Hangouts Chat, Hangouts Meet, Google Talk
- Jamboard
- Keep
- Sites
- Vault

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 You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, CMS may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account, although this should not be needed.

When a student 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 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 my child share information with others using the G Suite for Education account?

CMS may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. Although most work will only be shared internally between teachers and their classes, from time to time classes will produce work that is shared publicly. When users share information publicly in this way, it may be picked up and displayed by search engines, such as Google and accessed by users all across the internet.

Will Google disclose my child's personal information?

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

- **With parental or guardian consent.** Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- **With** CMS**.** 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, organizations 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 do I have as a parent or guardian?

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 the IT Manager at CMS. 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 David Todd at davidtodd@cundallmanor.org.uk 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 (at https://www.google.com/edu/trust/), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html)

APPENDIX 1– Staff Only

Use of mobile phones

- While it is recognised that members of staff may need to use their own telephone to contact each other, or relay information regarding expected arrival times from trips, any contact with parents or pupils should be undertaken through the school telephone system or using school mobile telephones, i.e. parents and pupils should not contact members of staff on their personal mobile phones. All calls to staff regarding school business should be directed through the main school telephone number.
- Staff must not use their own mobile telephones for taking photographs of children.
- Mobile phones should not be used when teaching, unless in an emergency.
- CMS has a number of mobile phones which are available for staff to use when on school trips. These phones are only to be used for pupil/ parent contact and emergency use.
- Pupils who bring mobile phones to school should only use them in case of emergency and should not use them during lesson times, unless otherwise indicated by the supervising member of staff.
- Mobile phones must not **by law** be taken into an EYFS setting
- Mobile phones must not **by law** be used while driving

Staff use of internet

- Use of the internet on school premises should principally be for school use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of e-mail on school business.
- Use of the school's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is prohibited.
- The school recognises that information can now be accessed online through the 'streaming' of data, i.e. radio, television, music, etc. Teachers and administration staff should only access streamed information if it is of educational interest to a lesson or to its planning. For example, using BBC iPlayer is acceptable if it is in the interest of the class and related lessons. Streaming music for personal use is discouraged. This is due to the streaming process placing demands on the schools internet bandwidth; as a result the internet can become slow for all users. Streaming data for personal use is not authorised.
- Teachers should not be accessing the internet for personal reasons whilst teaching children.
- Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. If accessed accidentally users should report the incident immediately to a member of the SMT or IT Manager, so the incident can be logged.
- Staff should not use any school computer to access social networking sites, such as Facebook, Twitter, etc, due to the potential virus risk these sites can carry. Any damage caused to school computer equipment as a result of such misuse is the responsibility of the member of staff, who may be asked to compensate the school.
- The school recognises that many staff will actively use Facebook, Twitter, and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to post information or discuss issues relating to children or other members of staff via these networks. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.
- Staff should be aware of the latest Teachers Standards available here: https://www.gov.uk/government/publications/teachers-standards
- Any photos or videos taken during **any** school activity should not be put on public display or published anywhere on the internet (including social networking sites such as Facebook) unless for school promotional purposes and with regard to pupils for whom the parents have given permission.
- It is **never** acceptable to accept a 'friendship request' from pupils at the school. In almost all such cases the pupils will be breaching the terms and conditions of use of those networks and the member of staff will be compromising themselves in respect of Child Protection Procedures. It is also extremely inadvisable to accept as friends ex-pupils who are still minors. If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgement at all times.
- Setting a high security level on social networking sites as advisable.

- Staff must not access websites that incite radicalisation or compromise the fundamental British values held by the school.
- Staff must log onto the school network using their personal user name and password only. Staff must not access the school network using the administrator user name and password or any other user name.
- Staff must not download software onto the school network before first liaising with the IT Manager to check for suitability. Software that is installed and is deemed not necessary for use in the school context will be deleted, i.e. iTunes, mobile telephone software, games, etc.
- Staff must ensure they log off after they have finished their session and leave the workstation in a tidy manner.
- Staff will ensure that they lock their workstation if left unattended to avoid unauthorised access to staff drives or school e-mails.
- Staff will not use the network in any way that would disrupt use of the network by others.
- Staff should not introduce "USB drives" or other portable devices into the network without having them approved and checked for viruses by the ICT Manager.
- School resources, such as software, etc. are for the use of staff and pupils within the school premises only and should **not** be taken home for personal use.

Use of portable computer systems, USB sticks or any other removable media

- If sensitive data, such as children's details and report comments, is stored on a portable device it should be encrypted or password protected. Other data, such as lesson plans and resources, may be stored on unencrypted devices.
- Staff should ensure all data is stored and used in compliance with the DPA 2018. More details on this can be found in our documentation regarding GDPR or at this site https://www.gov.uk/data-protection

Use of digital images

- Any photos or videos taken by teachers, other adults (including parents), and the children themselves during ANY school activity (including educational visits) should not be put on public display or published anywhere on the internet (including social networking websites).
- The above excludes the publication of photos on the CMS website, within the school newsletter, for the purpose of school related publicity, and where used by the school for educational/display uses, where the parents have given express permission to the school for them to do so.

Use of school hardware – laptops, cameras, recording equipment, etc.

- Use of school laptops, cameras, video cameras and recording equipment is limited to activities directly related to school activity. They can be used during lessons, sporting activities, school visits and residential trips. They are not for personal use.
- All data must be transferred to the school network as soon as possible to ensure that data is saved and protected. Once copied to the network the data must be deleted from the recording equipment.
- If travelling with these hardware items, and they contain information relating to staff and pupils, i.e. address details, photographs or reports, ensure that files are encrypted and password protected.

Reviewed April 2020

NOTE
It should be understood by all staff, that this Code of Practice is in place to protect staff from potential risk in their use of ICT in their everyday
—