Orchard School

E-Safety/Online Safety Policy

15th September 2021

Approved by Sandra Fox

The E-safety Policy/Online Safety Policy will be reviewed annually with the next review being September 2022.

Orchard School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practice good e-safety/ online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety/online safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

Educating all members of the school community on the risks and responsibilities of e-safety/online safety falls under the school's duty of care. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, in on-line learning and to provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety/online safety is a whole-school issue and responsibility. This policy should also be read in conjunction with the **Remote Learning Policy.**

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in other policies relating to our school including the **Child Protection Procedures and Safeguarding Policy, Cyber Bullying, Behaviour Policy** and the **Anti-Bullying Policy** and further policies relating to pupil behaviour and bullying.

AIMS

The school aims to:

- have robust processes in place to ensure the online safety of pupils, staff and volunteers.
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four key categories of risk

The school's approach to e-safety/online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

COMMUNICATING SCHOOL POLICY

This policy is available from the School Office and on the school website for parents, staff and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety/online safety is integrated into lessons in any circumstance where the internet or technology are being used, and during PDP lessons where personal safety, responsibility, and/or development are being discussed.

ROLES AND RESPONSIBILITIES

Head Teacher/Proprietor is responsible for:

- approving this policy
- ensuring that staff understand this policy, and that it is implemented consistently throughout the school.
- adhering to the terms on the acceptable use of the school's ICT systems and the internet.

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety in school, in particular:

- supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the Head Teacher, ICT staff and other staff, as necessary, to address any online safety issues or incidents.
- managing all online safety issues and incidents in line with the Whole School Child Protection Procedures and Safeguarding Policy.
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy and Anti-Bullying Polices.
- ensuring annual staff training on online safety.
- liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

Details of the school's DSL and deputy are set out in the Whole School Child Protection Procedures and Safeguarding Policy as well as relevant job descriptions.

The ICT Technician is responsible for:

- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems to ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

All staff, including contractors and agency staff, and volunteers are responsible for:

- maintaining an understanding of this policy
- implementing this policy consistently
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's Behaviour Policy and anti-bullying policies.
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy

arents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Healthy relationships – Disrespect Nobody

MAKING USE OF ICT AND THE INTERNET IN SCHOOL

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For pupils:

- Access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Access to subject experts, role models, inspirational people and organisations.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

Parents/carers will be asked to sign and return a consent form for pupil access. The school will maintain a current record of all pupils who are granted internet access. Lower and Upper School pupils will be asked to sign an 'Acceptable Use Agreement' (**Appendix One**) regarding the use of the school's ICT systems and the internet. Upon receipt of consent, students are provided with supervised internet access. Appropriate web filtering is provided and maintained by the ICT Technician.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to communicate with pupils, staff members and parents.

All staff must read and sign the Acceptable Use of ICT/Code of Conduct (**Appendix Two**) regarding the use of the school's ICT systems and the internet before using any school ICT resource/equipment. Staff should be aware that internet traffic could be monitored and traced to the individual. Discretion and professional conduct is essential.

For parents:

- A system is in place whereby instant communication can be made with parents and carers via email.

HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, the school will follow the procedures set out in the Behaviour Policy, this policy, the Whole School Child Protection Procedures and Safeguarding Policy and anti-bullying policies where appropriate. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff Code of Conduct and Acceptable use of ICT - Staff Information Systems Code of Conduct, Whole School Child Protection Procedures and Safeguarding Policy and Allegations of Abuse Against Staff Policy, where appropriate. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- children can abuse their peers online through:
    - abusive, harassing, and misogynistic messages
    - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - sharing of abusive images and pornography, to those who do not want to receive such content
    - physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse.
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputy undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in the Whole School Child Protection and Safeguarding Policy.

TEACHING AND LEARNING

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate.
- to use age-appropriate tools to search for information on line.
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Pupils who are found to have plagiarised will be disciplined.

The school acknowledges a responsibility to take all reasonable precautions to prevent access to inappropriate materials. Steps will be taken to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported (via the E-Safety/Online Safety Reporting Log **(Appendix Six**). Checks will take place by the school's IT technician to ensure that filtering services are working effectively.

EDUCATING PUPILS ABOUT E-SAFETY/ ONLINE SAFETY

Pupils are taught about e-safety/online safety as part of the curriculum in ICT, RSE and PDP. Details about the content which is taught can be seen in the school's Relationships and Sex Education Policy.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

EDUCATING PARENTS ABOUT E-SAFETY/ONLINE SAFETY

The school will raise parents' awareness of internet safety in letters, emails or other communications home, and in information via the school's website. This policy is also published on the school's website.

If parents have any queries or concerns in relation to E-Safety/Online safety, these should be raised in the first instance with the Head Teacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head Teacher.

MANAGING INFORMATION SYSTEMS

The school is responsible for reviewing and managing the security of the computers and internet network as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT technician. Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted.
- making sure that unapproved software is not downloaded to any school computers.
- files held on the school network will be regularly checked for viruses.
- the use of administration passwords to access staff computers.
- staff computers should be kept secure at all times and in a 'locked' status if on and not in use.
- portable media containing school data or programs will not be taken off-site without specific encryption or permission from a member of the senior leadership team.

If staff have any concerns over the security of their device, they must seek advice from the school's ICT Technician.

STAFF USING WORK DEVICES OUTSIDE SCHOOL

Work devices must be used solely for work activities.

All staff members must take appropriate steps to ensure their devices remain secure.

Every member of staff has an encrypted memory stick/USB drive. No other device can be used to store school personal data files unless the member of staff has an encrypted school laptop (it is important the hard drive is encrypted – this means if the device is lost or stolen no one can access the files stored on the hard drive by attaching it to a new device.) If the memory stick is taken off-site for example for school report writing the files on the memory stick **must not** be saved to an unencrypted computer at home. Any USB devices containing data relating to the school must be encrypted.

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use in the Staff Information Systems Code of Conduct.

Staff must ensure that their work device is secure, encrypted and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school this includes making sure the device locks if left inactive for a period of time, the device is not shared amongst family or friends and all anti-virus and anti-spyware software are kept up to date.

If staff have any concerns over the security of their device, they must seek advice from the school's ICT Technician.

For more information on data protection in school please refer to our **Data Protection Policy**.

EMAILS

The school's online learning platform is Google Workspace for Education. All teaching staff and all students in the school (with parental permission) have a G Mail email address.

Staff should be aware that school email accounts and G Mail accounts should only be used for school-related matters, i.e. for staff to contact parents, pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Pupils should be aware their school email accounts should only be used for school-related matters, i.e. to contact their teachers. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Staff should be aware of the following when using email in school:

- staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.
- emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should consider this when entering into any email communications.
- staff must tell the Head or one of the Assistant Heads if they receive any offensive, threatening or unsuitable emails from either within the school or from an external account. They should not attempt to deal with these themselves.
- the forwarding of chain messages is not permitted in school.

Pupils should:

- always use their G Mail accounts when in school and for online learning and these accounts should only be used for school-work related purposes.
- tell a member of staff if they receive any offensive, threatening or unsuitable emails from either within the school or from an external account. They should not attempt to deal with these themselves.

Pupils will be educated through their ICT lessons to identify spam, phishing and virus emails and attachments that could cause harm to the school computers or their personal accounts or wellbeing.

GOOGLE WORKSPACE FOR EDUCATION

Google Workspace allows students to access their work both at school and at home. Google Workspace is widely used in education and it is a safe online environment. Furthermore, most Post-16 centres or further education colleges as well as universities use Google Workspace or a similar system; so it is important especially for the students to learn how to work with these online tools safely and efficiently.

For more information please see the Google Workspace for Education *Notice to Parents* and *Privacy Notice* in Appendix Seven.

GOOGLE MEET

Google Meet is used for live-streamed lessons during periods of remote learning. Please refer to the Remote Learning Policy.

PUBLISHED CONTENT AND THE SCHOOL WEBSITE

The school website is viewed as a useful tool for communicating the school's ethos and practice to the wider community. It is also a valuable resource for parents, pupils, and staff for keeping up-to-date with school news and events.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information about staff or pupils will be published with the following exceptions. On the website are the details for contacting the School Office specifically the telephone numbers and email address, the names and email addresses for the proprietors, the Head Teachers of the two school sites and a phone number for the school's emergency out of hours contact. The name and contact number for the school's Designated Safeguarding Lead (DSL) are also on the website. The contact details for the DSL and the names and school email addresses of the Deputy DSL and the Mental Health Lead are in the school's *Child Protection Procedures and Safeguarding Policy* which is published on the school's website. In addition the name and school email address of the Head of Lower School is in the Safeguarding COVID-19 appendix.

POLICY AND GUIDANCE OF SAFE USE OF CHILDREN'S PHOTOGRAPHS AND WORK

Photographs and pupils' work bring the school to life, display the student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 2018, images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school, parents/carers will be asked to sign a consent form for processing pupils' personal data **(Appendix Five).** The school does this to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

USING PHOTOGRAPHS OF INDIVIDUAL CHILDREN

The vast majority of people who take or view photographs or videos of children do so entirely for innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications.
  - on the school website
  - in newspapers as allowed by the school.
  - in videos made by the school or in class for school projects.

- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities, which may pose a greater risk of potential misuse (for example, swimming activities); will focus more on the sport than the pupils.
- For public documents, including in newspapers, full names will not be published alongside images of the child (unless specific consent has been given by the parent or carer of the child or if the child is over 13 and capable of making the decision). Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as sports days must be used for personal use only.
- Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school, please refer to our school **Child Protection Procedures and Safeguarding Policy**.

SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programs. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school.

Social media sites have many benefits for both personal use and professional learning; however, both staff and pupils should be aware of how they present themselves online. Students are taught through ICT lessons and PDP about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows these rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and act appropriately.
- Staff members and volunteers, employed by Orchard School to undertake duties in any capacity, must not befriend pupils on social networking sites. This applies to former pupils as well who are under the age of 18.

MOBILE PHONES AND PERSONAL DEVICES

Please also read the *Mobile Phone and Smart Technology* Policy for further information. The term 'mobile phones' refers to the use of mobile and smart technology).

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make pupils and staff more vulnerable to cyber-bullying.
- they can be used to access inappropriate internet material.
- they can be a distraction in the classroom.
- they are valuable items that could be stolen, damaged or lost.
- they often have integrated cameras, which can lead to child protection, bullying and data protection issues.

Any pupil that brings a mobile phone or personal device into school is agreeing that they are responsible for handing it in. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.

Use of mobile phones and smart technology by pupils

The pupils are only allowed to access the internet during lesson times and on school devices. The school network is password protected and the pupils are not allowed to know the password. Pupils are not allowed their mobile phones during the school day – mobile phones are handed in at the start of Registration and returned to the pupils at the end of the school day. Pupils are also not allowed to have any personal devices such as electronic tablets in school. Pupils are given sanctions if these devices are not handed in at Registration.

Pupils are allowed to bring mobile phones with them on the school mini-buses but these have to be handed in at the start of Registration. Each pupil is allocated a jiffy bag in which they place their phone and then all phones for the year group are placed in a zipped bag and kept safe in the School Office during the day. The teacher who teaches each group last lesson hands back the mobile phones to pupils at the end of the school day.

Pupils are sometimes allowed their mobile phones at the direction of the teacher on educational trips and on residential trips. Pupils must adhere to the school's code of conduct/acceptable use agreement for mobile phone and smart technology use.

Sanctions

If a pupil is in breach of this policy.

- The phone will be confiscated for the remainder of the day. (Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006). Pupils are given lines to write as a sanction for having their phone on them in school, the number of lines increases for repeat offences.
- Depending on the circumstances the school's Behaviour Policy and Child Protection Procedures and Safeguarding Policy may also be implemented.

Staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate. Such conduct includes, but is not limited to:

- Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
- Upskirting
- Threats of violence or assault
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation
- Pupils under no circumstances are allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession, it will be confiscated. The breach of rules will be reported to the appropriate awarding body and may result in the pupil being prohibited from taking that exam and/or all other exams by the awarding body.

Staff

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room).
A member of staff may use their phone during contact time if they need to call another staff member for assistance following an incident in school, on the playground or on the school field.

Data Protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information.
Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it is necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

Using mobile phones for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work.

Such circumstances may include, but are not limited to:

- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil
- Refrain from using their phones to contact parents. If necessary, contact must be made via the School Office or by a school mobile phone.

Work Phones

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

Staff must:

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

Sanctions

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

CYBER-BULLYING

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, the topic is covered as part of the PDP curriculum to ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. Pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Cyber-bullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies in place to prevent and tackle bullying are set out in the school **Anti-Bullying Policy** and **Cyber-Bullying Policy**. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of cyber-bullying does arise, the school will follow its anti-bullying procedures. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

MANAGING EMERGING TECHNOLOGIES

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to develop appropriate strategies for dealing with new technological developments.

PROTECTING PERSONAL DATA

Orchard School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of how the data is collected, what is collected, and how it is used. Test results, attendance and registration records, special educational needs data and any relevant medical information are examples of the type of data that the school needs. Through effective data management, we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and pupils.

In line with the Data Protection Act 2018, and following principles of good practice when processing data, the school will ensure that data is:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed;
- Processed in a way that ensures it is appropriately secure.

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information on to external authorities, for example, the local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection read the school's **Data Protection Policy**.

EXAMINING ELECTRONIC DEVICES

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

LINKS WITH OTHER POLICIES

This E-Safety/Online Safety policy is linked to our:

- Whole School Child Protection Procedures and Safeguarding Policy
- Behaviour policy, Cyber-Bullying and Anti-Bullying Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints procedure

SUPPORTING DOCUMENTATION

The following documentation is held on file in the school office in support of the 'Orchard School E-Safety/Online Safety Policy'.

Appendix 1 - Acceptable Use Agreement (Lower & Upper School)

Appendix 2 - Acceptable Use of ICT - Staff Information Systems Code of Conduct

Appendix 3 - Consent Form for Processing Pupils' Personal Data

Appendix 4 - Orchard School E-Safety/Online Safety Rules

Appendix 5 - Parental Consent – E-Safety/ Online Safety Rules

Appendix 6 - E-Safety/Online Safety Reporting Log

Appendix 7 – Google Workspace for Education Information for Parents and Carers and Privacy Notice

Appendix One

Orchard School
Lower and Upper School Acceptable Use Policy Agreement

(This policy 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).

I understand that I must use school ICT systems, Google Workspace for Education and the internet in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will always use the school's ICT systems for educational purposes (the term 'school systems' includes the use of the computer systems and devices in school and the school's online learning platform which is Google Workspace for Education).
- I will use the internet in school responsibly and I understand I can only use the internet in school when a teacher is present and with his/her permission.
- I will keep my G Mail/ Google Classroom password secure – I will not share it, nor will I try to access another person's G Mail or attempt to log-in to Google Classroom using another person's account.
- If I attend a 'live-streamed' lesson through Google Meet in the event of remote learning I will be in a suitable location of my house and I will be wearing suitable clothing (for example not pyjamas).
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, educational details, gender etc).
- I will not arrange to meet people off-line who I have met online.

- I will immediately report to my teacher or any member of staff in school any unpleasant or inappropriate material, messages, or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials that are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails without first checking with a teacher, unless I know and trust the person/organisation who sent the email. If I have

any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs) I will not open it.

- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- I will not access any inappropriate websites including: social networking sites, chat rooms and gaming sites in school at any time.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that, the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include detentions, suspensions and contact with parents.

I have read and understand the above and agree to follow these guidelines when:

- I use the school system and devices (both in and out of school).
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school.

Signed .....

Print name: …….. Date .....

Appendix Two

Orchard School Acceptable use of ICT - Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E-Safety/Online Safety Policy for further information and clarification.

This code of conduct is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems (the term 'school systems' includes the use of the computer systems and devices in school and the school's online learning platform which is Google Workspace for Education) and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

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

Acceptable use of ICT/ Code of Conduct Policy Agreement:

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- I will not use the school systems in any way which could harm the school's reputation.
- I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology.
- I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email) out of school, and to the transfer of digital personal data out of school. Personal digital data taken out of school should be stored on encrypted laptops or encrypted memory sticks.
- I understand that school information systems may not be used for private purposes, without specific permission from the school Head Teacher.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other person's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not access social networking sites or chat rooms.
- I will not befriend pupils on social networking sites or engage in any on-line activity that may compromise my professional responsibilities. This applies to former pupils as well who are under the age of 18.
- I will only communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner. ***Note: any contact with parents via telephone should be logged via the school office and copies of any email communication should be forwarded to the Head Teacher.***
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will respect copyright and intellectual property rights.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety/online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content, they access or create.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up.
- I will not install any unauthorised software/programs of any type, or connect unauthorised hardware or devices to the school's ICT system, nor will I try to alter computer settings without permission.

- I will not try to upload, download or access or attempt to access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will also not create, share, link or send such material. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will not share my password with others or attempt to use another person's details.
- I will not access, modify or share data that I am not allowed to access, modify or share.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand the school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to the school's disciplinary procedures, a referral to the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name:

Signed: Date:

Appendix Three

Orchard School

Consent form for processing pupils' personal data

At Orchard School we use information about your child/children in a number of different ways, and we would like your consent for some of the ways we use this personal data.

In particular we sometimes take photographs of the pupils. We use these photos to help us to give people an idea of what life at our school is like, for example in the newsletter, in local newspapers and in internal displays in school.

If you are not happy for us to use the information in the ways we list below, that is no problem – we will accommodate your preferences.

Similarly, if you change your mind at any time, you can withdraw or grant consent. Please let us know by emailing office@theorchardschool.co.uk, calling the school on 01427 880395, or in person at the School Office.

If you have any other questions, please get in touch.

Please tick the relevant box(es) below, sign and return this form to school.

Child's name:

Name and relationship to child:

Signature:

Date:

Taking of photographs	Tick (√)
I am happy for the school to take photos of my child.	
I am happy for the school to employ the services of a professional photographer to take individual and sibling photographs of my child/children once a year.	
I am happy for the school to employ the services of a professional photographer to take class, sport teams and whole school photographs once a year.	
I am happy for photographs of my child to be taken by a professional photographer if she/he attends the Year 11 Prom.	

Using of photographs	
I am happy for photos of my child to be used in internal displays.	
I am happy for photos of my child to be used in the school newsletter.	
I am happy for photos of my child to be used in printed school materials, for example, the school prospectus.	
I am happy for photos of my child to be used on the school website.	
I am happy for photos of my child to be used in the media, for example local newspapers.	
I am happy for photos of my child to be included in programmes e.g. Drama and Music productions, the Christmas production	
I am happy for photos of my child to be selected for inclusion on the front cover of the Senior School Student Planner	
Taking and use of videos	
I am happy for the school to take video footage of my child.	
I am happy for the school to use video footage internally in school e.g. during the end of year review service.	
I am **NOT** happy for the school to take or use photos of my child.	
I am **NOT** happy for the school to take or use video footage of my child.	

Please note that consent is not needed to take photographs or video footage when it is required to form part of the curricular records, like in the Early Years Foundation Stage, or as an element of assessment in a course like Drama.

Appendix Four

Orchard School E-Safety Rules

These E-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

The school owns the computer network and can set rules for its use.

- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the Head Teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix Five

PARENTAL CONSENT

Orchard School E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the E-Safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school E-safety/Online Safety rules and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Please sign this consent and return to school.

Signed: ..... Date: .....

Please print name:.....

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, E-safety education to help them understand the importance of safe use of technology and the Internet - both in and out of school.

Appendix Six

Reporting Log **Year:**						
Date	Time	Incident	Action taken		Incident reported by:	Signature
			What?	By whom?		

Appendix Seven

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

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

Orchard School does not allow students to access Additional Services from their Google Workspace for Education accounts.

Google provides information about the data it collects, as well as how it uses and discloses the information it collects from Google Workspace for Education accounts in its Google Workspace for Education Privacy Notice. You can read that notice online at https://workspace.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, Orchard School 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 Google Workspace for Education account.

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 Google Workspace 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 Google Workspace for Education users in primary and secondary schools, Google does not use any user personal information (or any information associated with a Google Workspace for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using a Google Workspace for Education account.

Can my child share information with others using the Google Workspace for Education account?

We 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. When users share information publicly, it may be indexable by search engines, including Google.

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 Google Workspace for Education schools.
- With Orchard School. Google Workspace 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 Google Workspace 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 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 do not provide your consent, we will not create a Google Workspace 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 Google Workspace for Education, you can access or request deletion of your child's Google Workspace for Education account by contacting the School Office. 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 Google Workspace 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 Google Workspace for Education accounts or the choices available to you, please contact the School Office. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the Google Workspace for Education Privacy Center (at https://www.google.com/edu/trust/), the Google Workspace for Education Privacy Notice (at https://workspace.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).

The Core Google Workspace for Education services are provided to us under Google Workspace for Education Agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html

Google Workspace for Education Privacy Notice

This privacy notice is meant to help you understand what data we collect, why we collect it, and how you can manage your information while using a Google Workspace for Education account.

Google Workspace for Education facilitates learning and collaboration among students (and parents), educators, and school admins. Google Workspace for Education includes two categories of services, both described in this privacy notice. The distinction is important because the scope of the services and how the data is processed in these services differs.

Google Workspace for Education core services are listed in the Services Summary and include Gmail, Calendar, Classroom, Assignments, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Chat, Meet, Vault, and Chrome Sync.

Google Workspace for Education additional services include services we make generally available for all consumers, such as Google Search, Maps, and YouTube, which Workspace for Education users may have access to with their Workspace accounts.

This document provides the key information about both types of services. If you want to learn more, you can find additional information and examples in the following documents that also apply to Google Workspace for Education accounts. The Google Cloud Privacy Notice provides more information about data that we process while providing the core services, and the Google Privacy Policy provides more information about data that we process in additional services.

Your information: what we collect & how it is used

A Google Workspace for Education account is a Google Account created and managed by a school for use by students and educators. The account can be used for both core and additional services, and the information that we collect and store in your account is treated as personal information. Admins manage how students use core and additional services with their Google Workspace for Education accounts, including obtaining parental consent for the additional services that they choose to enable for students. Learn more about core and additional services for Google Workspace for Education users.

Core Services

As students, educators, and admins use Workspace core services, we collect two types of data:

- Things that you provide or create through core services (customer data)
- Information we collect as you use core services (service data)

There are no ads shown in Google Workspace for Education core services. Also, none of the personal information collected in the core services is used for advertising purposes.

Things that you provide or create through core services

We receive customer data through the core services and process it according to the school's (the customer's) instructions. This *customer data* includes anything submitted, stored, sent or received through core services by you or your school.

When a Google Workspace for Education account is created, the school provides Google with certain personal information about its students and educators that includes the user's name, email address, and password. Schools can also choose to share things like a user's secondary email

address, phone number, and address. And users can also add information to their account, such as an additional phone number and profile photo.

Things that you might create through the services include emails that you write and receive while using Gmail or documents that you draft and store in Drive.

Customer data is used to provide the core services, for example, Google processes your email address to send and deliver messages between teachers and students.

Information we collect as you use core services

As described more fully in Google's Cloud Privacy Notice, we also collect service data through the core services, including:

- **Your activity while using the core services**, which includes things like viewing and interacting with content, people with whom you communicate or share content, and other details about your usage of the services.
- **Your apps, browsers & devices.** We collect info about the apps, browser, and devices you use to access our services. This information includes browser and device type, settings, unique identifiers, operating system, mobile network information, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date and time of your request.
- **Your location information.** We collect info about your location as determined by various technologies such as IP address and GPS.
- And for admins, payments and transaction data and direct communications with us.

Service data is primarily used to deliver the services that schools and students use, but it is also used to maintain and improve the services; make recommendations to optimize the use of the services; provide support; protect our users, the public, and Google; and comply with legal obligations. See the Google Cloud Privacy Notice for more information.

Additional Services (Orchard School only uses the Google Workspace for Education core services)

As students, educators, and admins use additional services, we collect two types of data:

- Things that you provide or create through additional services
- Information we collect as you use additional services

Things that you provide or create through additional services

As described more fully in Google's Privacy Policy, we collect information when students and educators use the additional services, including things that you provide to us, content that's created or uploaded, and content that's received from others. For example, if you sign in to an additional service with a Workspace account, we will use your Workspace name and profile information to identify your account. You can also choose to save your content with Google, things like photos and videos.

Information we collect as you use additional services

Google's Privacy Policy also describes the information we collect as you use our additional services, which includes:

- **Your activity while using additional services,** which includes things like terms you search for, videos you watch, content and ads you view and interact with, voice and audio information when you use audio features, purchase activity, and activity on third-party sites and apps that use our services.
- **Your apps, browsers & devices.** We collect the info about your apps, browser, and devices described above in the core services section.
- **Your location information**. We collect info about your location as determined by various technologies including: GPS, IP address, sensor data from your device, and information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices. The types of location data we collect depend in part on your device and account settings.

Why we collect data

The data we collect in the additional services is used across our services to deliver, maintain, and improve our services; develop new services; provide personalised services; measure performance; communicate with you; and protect Google, our users, and the public. See the Google Privacy Policy for more details.

Some additional services show ads. But if you're using your Google Workspace for Education account in primary and secondary schools (K-12), we do not show you personalised ads, which means we do not use information from your account or past activity to target ads. However, we may show ads based on general factors like your search query, the time of day, or the content of a page you're reading.

Sharing your information

When you share your information

Your school's admin may allow students to access Google services, such as Google Docs and YouTube, that have features that allow users to share information with others or publicly. For example, if you leave a review in Google Play, your name and photo appear next to your activity. And if you share a photo with a friend who then makes a copy of it, or shares it again, then that photo may continue to appear in your friend's Google Account even after you remove it from your Google Account. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When Google shares your information

We do not share your personal information with companies, organisations, or individuals outside of Google except in the following cases:

- **With your school's admin**: Your admin and resellers who manage your Workspace account will have access to your information, including your password and information stored in your account
- **With your consent:** We will share personal information outside of Google when we have your consent.
- **For external processing**: We may share personal information with our affiliates and other trusted businesses or persons to process it for us, based on our instructions and in

compliance with our Privacy Policy, the Google Cloud Privacy Notice, and any other appropriate confidentiality and security measures.

- **For legal reasons**: We may also share personal information if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary for legal reasons, including complying with enforceable governmental requests and protecting you and Google.

Your privacy controls

We provide a variety of controls that enable students and parents to make meaningful choices about how information is used in Google services. Depending on the settings enabled by your school's admin, students can use settings like Google activity controls, to manage their privacy and information. We provide additional information for parents, students, and admins in the Google Workspace for Education Privacy Center.

School admins also have service controls that can allow you to manage personal information, including limiting its further collection or use. If you or your child has a Google Workspace for Education account, contact your admin to:

- access your personal information
- limit access to features or services
- delete personal information in services or delete your entire account

About this policy

This Notice is intended to provide the key information about our collection and use of data for Google Workspace for Education users, and is consistent with the Google Privacy Policy and the Google Cloud Privacy Notice. In cases that specific commitments differ, this privacy notice takes precedence followed by the Google Cloud Privacy Notice and the Google Privacy Policy. For example, the Google Privacy Policy has a description of personalised ads that isn't relevant to Google Workspace for Education users in primary and secondary schools (K-12), and this notice clarifies that we don't show personalised ads to those students.

Contact Us

Please visit the Google Workspace for Education Privacy Center for answers to most questions. Also see our Privacy Help Center for questions about privacy and Google's services.

If you are a parent:

- Contact your school admin if you have questions regarding the management of Google Workspace for Education accounts or the use of information by your child's school
- Or contact Google about the information in this notice

If you are an admin, contact Google about the information in this Notice by submitting the contact form while signed in to your admin account.

Google, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

(650) 253-0000