Lodge Farm Primary School
Online Safety Policy

Online Safety Lead	Emma Walton
Date of issue:	September 2022
Review date:	September 2023

Contents

1. Introduction

Lodge Farm school recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

2. Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety leader in this school is Emma Walton.
All breaches of this policy must be reported to Emma Walton and Helen Turner (Headteacher).
All breaches of this policy that may have put a child at risk must also be reported to the DSL, Helen Turner (Headteacher), Alexa Simpson (Assistant Head) and Angie Smith (Assistant Head) Jo Jones and Mary Bull.
Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. **If, however, they have any access to the school network and equipment then they must adhere to the school's online safety procedures and acceptable use agreements.** If an organisation doesn't have a policy, then school can support them to get one in place.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, GDPR, health and safety, behaviour, anti-bullying, PSHCE/RSE and Retention of Information.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or Governor Hub for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Emma Walton (Online safety leader).

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with

the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.

- When working with pupils, searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to

organisations connected to other networks except where permission has been given to the school

- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Online Safety leader and/or Headteacher.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the headteacher. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Year 6 pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes during the school day. All devices must be switched off on entry to the site and handed to the class teacher during registration. If they have been given permission to bring their mobile phone to school, they will only use it at the end of the school day once they have left the school site.

Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles may only be used to access school emails when logging in directly through Herts Grid and not through the use of quick access apps.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the headteacher before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the

incident immediately to the first available member of staff, the DSL, Helen Turner (Headteacher), Alexa Simpson (Assistant head), Angie Smith (Assistant Head) Jo Jones, Mary Bull or Emma Walton (Online Safety leader). Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of

respecting other people's information, reputation and images

- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

Anti-Radicalisation and Counter-Extremism

Staff will sign a register to show that they have read and fully understand their responsibilities regarding The Prevent Duty document (June 2015). They have also be directed to read 'How Social Media is used to encourage travel to Syria and Iraq' document (see web link below).

'It is essential that staff are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified.' (pg5)

'…schools and childcare providers should be aware of the increased risk of online radicalisation, as terrorist organisations such as ISIL seek to radicalise young people through the use of social media and the internet.' (pg6)

'Schools and childcare providers should have clear procedures in place for protecting children at risk of radicalisation. These procedures may be set out in existing safeguarding policies.' (pg6)

'IT policies….

…the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

…schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum…..

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.' (pg8)

The Prevent Duty: Departmental advice for schools and childcare providers June 2015

For more information refer to the Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance
https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

All staff and governors, including new staff and governors as part of their induction before having contact with pupils, are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement annually (Appendix A).

Occasional visitors and organisations working with children based on the school premises are required to read the Occasional Visitors Acceptable Use Agreement and Code of Conduct on the front of the Visitor's sign in book in the school office before entering the school (Appendix B).

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process.

All parents are asked to consent to the school setting up a G Suite for Education account for their child (Appendix C).

The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and separate online safety letters.

Parents/carers are asked on an annual basis to read and discuss with their child the Acceptable Use Agreement (Appendices D and E). This is then discussed in every class. In KS2, each child signs to confirm they have read and understood the agreement, whereas the teacher signs on behalf of the children in EYFS and KS1.

The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe. A Parent/Carer Social Media Acceptable Use Agreement (Appendix F) and a Summary of key parent/carer responsibilities (Appendix G) explains the school's expectations and pupil and parent/carer responsibilities. Parents are advised that by sending their child/ren to Lodge Farm School, they agree to adhere to the rules outlined in the agreement.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

Appendix H outlines the process for responding to online cyberbullying incidents and Appendix I provides guidance for staff on preventing and responding to negative comments on social media.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Online safety incident recording formats are provided in appendices J, K and L.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

9. Appendices of the Online Safety Policy

A. Staff, Governors and Visitors Acceptable Use Agreement and Code of Conduct

B. Occasional Visitors Acceptable Use Agreement and Code of Conduct

C. G Suite for Education parental consent letter

D. EYFS and KS1 Pupil Acceptable Use Agreement and Online Safety Rules

E. KS2 Pupil Acceptable Use Agreement and Online Safety Rules

F. Parent/Carer Social Media Acceptable Use Agreement

G. Online safety policy guide - Summary of key parent/carer responsibilities

H. Guidance on the process for responding to cyberbullying incidents

I. Guidance for staff on preventing and responding to negative comments on social media

J. Online safety incident reporting form

K. Online safety incident record for staff completion

L. Online safety incident log

Appendix A

Staff, Governors and Visitors Acceptable Use Agreement and Code of Conduct

**Staff refers to all staff on the payroll.*
**Visitors refers to regular visitors to the school such as supply teachers.*

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff and governors are aware of their professional responsibilities when using any form of ICT. All staff and governors are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with Emma Walton (Online Safety Lead) or Helen Turner.

- I will only use the school's email, Internet, network, website and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any usernames or passwords provided to me by the school or other related authorities. If my password is compromised, I will change it.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- I will not use personal electronic devices (including smart watches) in public areas of the school, except the staffroom, unless approved by the Online Safety Lead or Headteacher, between the hours of 8.30am and 3.30pm.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that all electronic communications with pupils, staff and outside agencies are compatible with my professional role.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop.
- I will not install any hardware or software without permission of the school.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any accidental access to, or receipt of inappropriate materials, filtering breach or equipment failure to the Online Safety Lead or IT technician.
- I will not use personal digital cameras, camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store such images or videos at home.
- Images of pupils/staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will check copyright and not publish or distribute any work including images, music and videos, that are protected by copyright without seeking the author's permission.

- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- ***Teachers:*** I will embed the school's approach to online safety in every computing lesson and other lessons as appropriate.
- I understand that all my use of the Internet and other related technologies, in school, can be monitored and logged and can be made available, on request, to the Online Safety Coordinator or Headteacher.
- I will not upload or add any images, video, sounds or text linked to or associated with the school or its community onto social media.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.
- I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this Acceptable Use Agreement and Code of Conduct and to support the safe and secure use of ICT throughout the school.

Please sign the staff sheet to agree that you have read and fully understand your responsibilities regarding your use of ICT as outlined in the above Acceptable Use Agreement in relation to Lodge Farm Primary School.

Appendix B

Occasional Visitors Acceptable Use Agreement and Code of Conduct

**Occasional visitors refers to visitors that are in school for a one –off occasion such as a supply teacher that is not regularly used by the school, a visiting speaker or students that are helping for single days.*

On signing the visitor's book, you agree to:

- only log onto the school network with the username and password provided for you;
- use the Internet in a responsible and safe manner;
- refrain from using your personal mobile phone or other device in any public place within the school, except the staffroom;
- not take any photographs, unless directed to by a member staff for the purpose of providing evidence for a lesson;
- report any suspected misuse or concerns about online safety whether by pupils or staff, to the headteacher of their representative;
- not take any information on pupils or staff off site unless specific permission has been given by the headteacher or their representative;
- not publishing any information online that may be offensive to staff or pupils, or may bring the school into disrepute.

Appendix C

Lodge Farm Primary School
Mobbsbury Way
Chells
Stevenage
Herts SG2 0HR

Tel: 01438 236600 Fax: 01438 236601
Information Line: 08453 316191

"Learning in mind, community at heart"

email: admin@lodgefarm.herts.sch.uk
www. lodgefarm.herts.sch.uk

Headteacher: Helen Turner

G Suite for Education Parental Consent

G Suite for Education is a set of education productivity tools used by tens of millions of students and teachers around the world. Its Google tools include Gmail, Calendar, Docs, Classroom and much more. Please be assured that Lodge Farm's G Suite for Education account has been created so that our children can only communicate with other Lodge Farm users.

This letter requests **your consent** for the school to provide and manage a G Suite for Education account for your child/ren.

The notice attached provides answers to common questions about what Google can and cannot do with your child/ren'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 the information carefully and sign the consent form below to indicate that you have read the notice and that you give **your consent** for the school to manage and provide a G Suite for Education account for your child/ren. Please return the consent form to your child/ren's class teacher as soon as possible. Once you have done this, your child will receive their username and password details.

If you do not provide your consent, we will **not** create a G Suite for Education account for your child/ren. If you do not give your consent for your child/ren to use the Google services, your child/ren's teacher(s) **will** provide them with other software or paper-based resources to complete their tasks and to collaborate with their peers in lessons. Your child/ren will receive the same teaching and learning opportunities as their peers. However, not being able to use the Google

services could impact their educational experiences of the broader curriculum, their digital communication and their development of digital citizenship skills.

If you have any questions, please do not hesitate to contact the school. Thank you in advance for your support in enabling Lodge Farm to become a G Suite for Education school.

Helen Turner — Headteacher

Emma Walton — Computing and Online Safety Lead

Parent/Carer consent form for G Suite for Education

Please return to your child's class teacher

I give permission for Lodge Farm to create and maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below.

Full name of child: _____

Printed name of parent/carer: _____

Signature of parent/carer: _____

Date: _____

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 - email
- Google+ - a social networking site
- Calendar
- Chrome Sync
- Classroom – paperless tasks and collaborative work
- Cloud Search – search engine
- Contacts
- Docs, Sheets, Slides, Forms - similar to Microsoft programs
- Drive – file storage and synchronisation
- Groups – discussion groups
- Hangouts, Hangouts Chat, Hangouts Meet, Google Talk – communication tools
- Jamboard – interactive whiteboard
- Keep - notetaking
- Sites – wiki and web page creation tool
- Vault - data tool

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 which is attached or 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, Lodge Farm 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. **Please note that at this time, the children's G suite accounts will only be used in school accessed using the Chromebooks. As such, children's telephone numbers will not be required for account recovery as this refers to use on personal devices.**

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 a 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?

Lodge Farm 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, organisations and individuals outside of Google unless one of the following circumstances applies:

- **With parental or guardian consent.** Google will share personal information with companies, organisations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools. **This refers to G Suite accounts being accessed using personal devices and as such, Lodge Farm will not request your consent for this.**
- **With Lodge Farm.** 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 school. 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 the school. 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) The school has accepted the Data Processing Amendment (see https://support.google.com/a/answer/2888485?hl=en) and the Data Processing Amendment (at https://www.google.com/intl/en/work/apps/terms/dpa_terms.html).

Google for Education

Taken from https://gsuite.google.com/terms/education_privacy.html

G Suite for Education Privacy Notice

This Privacy Notice is meant to help G Suite for Education users and parents understand what data we collect, why we collect it, and what we do with it. This Notice includes information about our privacy practices that are specific to G Suite for Education and summarizes the most relevant portions of the Google Privacy Policy, which provides additional examples and explanations that may be useful. We hope you will take the time to read this Notice and the Google Privacy Policy, which both apply to G Suite for Education accounts.

Information we collect

A G Suite for Education account is a Google Account created and managed by a school for use by students and educators. When creating this account, the school may provide Google with certain personal information about its students and educators, which includes a user's name, email address, and password in most cases, but could also include secondary email, phone, and address if the school chooses to provide that information. Google may also collect personal information directly from users of G Suite for Education accounts, such as telephone number, profile photo or other information they add to a G Suite for Education account.

Google also collects information based on the use of our services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number of the user;
- log information, including details of how a user used our service, 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 we use information we collect

1. **In G Suite for Education Core Services**
2. The G Suite for Education Core Services ("Core Services") are listed in the Services Summary and include Gmail, Calendar, Classroom, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts, Vault, and Chrome Sync. These services are provided to a school under its G Suite for Education agreement and, as applicable, Data Processing Amendment. (Users and parents can ask their school if it has accepted the Data Processing Amendment.)

3. User personal information collected in the Core Services is used only to provide the Core Services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.
4. **In Google services generally**
5. Besides the Core Services, G Suite for Education users may have access to other Google services that we make generally available for consumers, such as Google Maps, Blogger, and YouTube. We call these "Additional Services" since they are outside of the Core Services.
6. The Google Privacy Policy describes fully how Google services generally use information, including for G Suite for Education users. To summarize, we use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer users tailored content, such as more relevant search results. We may combine personal information from one service with information, including personal information, from other Google services.
7. Google may serve ads to G Suite for Education users in the Additional Services. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with a G Suite for Education Account) to target ads, whether in Core Services or other Google services accessed while using a G Suite for Education account.

Learn more about Core and Additional Services for G Suite for Education users.

Information users share

A school 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. Our services provide users with various options for sharing and removing content.

Information we share

Information we collect may be shared outside of Google in limited circumstances. We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- **With user consent.** We will share personal information with companies, organizations or individuals outside of Google when we have user consent or parents' consent (as applicable).
- **With G Suite for Education administrators.** G Suite for Education administrators have access to information stored in the Google Accounts of users in that school or domain.
- **For external processing.** We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.
- **For legal reasons.** We will share personal information with companies, organizations or individuals outside of Google if we have 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, our users or the public as required or permitted by law.

We may share non-personal information publicly and with our partners – like publishers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

Transparency and choice

We provide a variety of user controls that enable G Suite for Education users to make meaningful choices about how information is used in Google services. Depending on the settings enabled by the school, users can use the various controls described in the Privacy Policy, such as Google activity controls, to manage their privacy and information. We provide additional information for parents, students, and administrators on the G Suite for Education Privacy Center.

Parental review and deletion of information

The parents of G Suite for Education users in Primary/Secondary (K-12) schools can access their child's personal information or request that it be deleted through the school administrator. School administrators can provide for parental access and deletion of personal information consistent with the functionality of our services. If a parent wishes to stop any further collection or use of the child's information, the parent can request that the administrator use the service controls available to them to limit the child's access to features or services, or delete the child's account entirely. Guidance for administrators on how to use service controls to accomplish this is available in the G Suite Help Center.

Interpretation of conflicting terms

This Notice is intended to provide the key information about our collection and use of data for G Suite for Education users, and is consistent with the Google Privacy Policy and the G Suite for Education agreement, which provide additional examples and explanations that may be useful. Where there are terms that differ, as with the limitations on advertising in G Suite for Education, the G Suite for Education agreement (as amended) takes precedence, followed by this Privacy Notice and then the Google Privacy Policy.

Contact us

If you have questions about management of G Suite for Education accounts or use of personal information by a school, please contact the G Suite for Education account administrator. If you have questions about our practices, please visit the G Suite for Education Privacy Center. Also see our Privacy Troubleshooter for more questions about privacy and Google's products and services. G Suite for Education administrators can contact Google about the information in this Notice by submitting the contact form while signed in to their administrator account. Parents can also contact Google about the information in this Notice.

Google

1600 Amphitheatre Parkway, Mountain View, CA 94043 USA

Phone: +1 650-253-0000

Appendix D

EYFS and KS1 Pupil Acceptable Use Agreement and Online Safety Rules

Think before you click

S 	I will only use the Internet and email with an adult.
A 	I will only click on icons and links when I know they are safe.
F 	I will only send friendly and polite messages.
E 	If I see something I don't like on a screen, I will always tell an adult.

I have read and talked about these rules with my teacher to help me to understand them.

Class: _____ **Class Teacher:** _____

Appendix E

KS2 Pupil Acceptable Use Agreement and Online Safety Rules

I will support Lodge Farm's approach to online safety by following these rules below. I know that they will keep me safe and help me to be fair to others.

- I will only use computing in school for my schoolwork and homework.
- I will keep my usernames and passwords secret and not share them with anyone else.
- I will only open, edit and delete my own files and not look at, or change other people's files without their permission.
- I will not bring files into school without permission or deliberately upload or add images, videos, sounds or text that could upset anyone in the school community.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will only use my class or individual school e-mail address when e-mailing.
- I will only e-mail people I know, or who a responsible adult has approved.
- The messages I send, or information I upload, will always be responsible, polite and sensible.
- If I receive a message I do not like, I will not respond to it. I will show a trusted adult.
- I will not open an attachment or download a file; unless I know and trust the person who has sent it or it has been approved by a responsible adult.
- I will not give out my full name, home address, phone number, send a photograph or video, or give any other information that could be used to identify me, my family or friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever met online, unless my parent/carer has given me permission and I take a responsible adult with me.
- I am aware that some websites and social networks have age restrictions (usually 13+) and I should respect this by not registering with them.
- If I have been given permission to bring my mobile phone to school, I will only use it at the end of the school day once I have left the school site.
- I will not bring a Smart Watch to school because I am not allowed to wear one during the day.
- I know that my use of technology, in school, can be checked and that my parents/carers contacted if a member of school staff is concerned about my online behaviour or safety.
- I know that the school may investigate incidents that happen outside of school which could have an effect on the school.
- I will participate responsibly in online safety lessons and activities, so I can continue to learn how to keep myself safe online and what I can do, or who I can tell, if something happens which does not make me feel safe.

I have read and talked about these rules with my class teacher and I understand how I can be responsible for my own online safety and be fair to others.

Class: _____ **Class Teacher: _____**

Date: _____

Appendix F

Lodge Farm Primary School
Mobbsbury Way
Chells
Stevenage
Herts
SG2 0HR

Tel: 01438 236600

Headteacher: Helen Turner

"Learning in mind, community at heart"

email: admin@lodgefarm.herts.sch.uk
www. lodgefarm.herts.sch.uk

DATE

Dear Parents/Carers,

Computing, including the Internet, e-mail and mobile technologies, has become an important part of our learning in school. We expect all children and their parents/carers to be safe and responsible when using any ICT.

Please find attached a copy of the 'Pupil Acceptable Use Agreement and Online Safety Rules' for EYFS and KS1 and KS2. These will be discussed in a Computing and Online Safety lesson with your child/ren next week. Please feel free to discuss the Acceptable Use Agreement with your child prior to the lesson but do not sign and send them into school.

If you have any concerns, or would like further explanation, please contact Mrs Walton or Miss Turner.

Parent/Carer Social Media Acceptable Use Agreement

The school's methods of communication include the prospectus, website, newsletters, letters and verbal communication. The statements below aim to make you aware of your responsibilities regarding your use of social networking, to ensure the online safety of all our pupils, parents/carers and staff at Lodge Farm Primary School.

- Parents/carers will not post pictures of pupils, other than their own child on social networking sites.
- Parents/carers will go through the official channels to make complaints, rather than posting them on social networking sites.
- Parents/carers will not post malicious or fictitious comments on social networking sites about any member of the school community.
- If parents/carers have a concern pertaining to the school, they will contact the school office to speak to a member of staff.
- Parents/carers will inform the school if they think there is an online safety issue related to a member of the school community.

Lodge Farm wishes to remind parents/carers that Facebook and other social media sites are only intended for users aged over 13. The school understands that it is very easy for young

people (or indeed adults) to enter an incorrect date of birth or false information to open an account.

We ask you to be diligent in monitoring your child's use of social media. As a school, if we discover that your child has a social media account, we will contact you and give you and your child the opportunity to close the account. If the account is not closed, we will contact the company directly to inform them of your child's actual age.

By sending your child/ren to Lodge Farm Primary School, you agree to support and follow our online safety policy as outlined in the Pupil Acceptable Use Agreements relevant for your child/ren's key stage. You also agree that you have read and fully understand your responsibilities regarding your use of social networking in relation to Lodge Farm Primary School.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Thank you in advance for your support.

Miss Turner
Head teacher

Miss Walton
Online Safety Lead

Appendix G

Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding the Online Safety Acceptable Use Agreement for pupils.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix H

Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix I

Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;

- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix J

Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident, please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the Online Safety leader and/or headteacher.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix K

Online safety incident record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Coordinator/DSL/ DSP/Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix L

Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety leader or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken
