Christ Church

Primary School

Starting the journey well

As a Church of England community school, we

believe we can impact God’s world for good,

grow in learning, love, wonder and faith and

seek together to flourish in the fullest way possible

E-Safety and Computing Policy 2022

Review Date: September 2023

Introduction

Key people / dates

Christ Church CE Primary School	Designated Safeguarding Lead (DSL) team	Jessica Williams
	Online-safety lead (if different)	
	Online-safety / safeguarding link governor	Tej Stride
	PSHE/RSHE lead	Jessica Williams
	Network manager / other technical support	Paul Moore
	Date this policy was reviewed and by whom	September 2022 Jessica Williams/Paul Moore
	Date of next review and by whom	Ella Heredge Thomas/Paul Moore July 2023

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leaders. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022(KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2021 and other statutory documents. It is designed to sit alongside our school's statutory Child Protections and Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these risks are mentioned in KCSIE 2022. Examples of which include child sexual exploitation; child criminal exploitation; radicalisation; sexual predation/grooming; and forms of Child-on-Child abuse. Technology often provides the platform that facilitates harm.

In past and potential future **remote learning and lockdowns**, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that some pupils may have missed opportunities to disclose abuse.

All staff should stay up to date with the latest news, risks, opportunities, best-practice and trends included on the LGfL DigiSafe blog, newsletter and their Twitter/Facebook channels.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible and understood by all. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers.
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Overview

Aims

This policy aims to:

- Set out expectations for all Christ Church CE Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope

This policy applies to all members of the Christ Church CE Primary School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher – Jessica Williams

Key responsibilities:

- Support technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised

- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Jessica Williams and Caroline Klejdys-Lord

Key responsibilities "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated"

- Work with technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Ensure an effective approach to online safety empowering our school to protect and educate the whole community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate.
- Liaise with staff (especially pastoral support staff, IT Technicians, SENCo and Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the head teacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are and submit for review to the governors.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance and in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents
- Communicate regularly with SLT and online safety governor to discuss current issues, review incident logs and filtering. Discuss how filtering and monitoring work and have been functioning/helping maintain e-safety.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged on myconcern in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site

- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware

Governing Body, led by Online Safety / Safeguarding Link Governor – Tej Stride

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2020)

- Approve this policy and strategy and subsequently review its effectiveness
- Ask about how the school has reviewed protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Ensure an appropriate **senior member** of staff, from the school **leadership team**, is appointed to the role of DSL with **lead responsibility** for safeguarding and child protection (including online safety). Ensure the appropriate time, funding, training, resources and support have been implemented.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and head teacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in school
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated in line with advice from the local three safeguarding partners, integrated, aligned and considered as part of the overarching safeguarding approach.
- Ensure appropriate filters and appropriate monitoring systems are in place, whilst taking care that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology.

All staff

Key responsibilities:

- Recognise that **RSHE** it is a whole-school subject requiring the support of all staff; online safety is part of this curriculum
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job
- Know who the Designated Safeguarding Lead and Deputy Safeguarding Leads are.
- Read Part 1, Annex A, Annex B – online safety resources
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents on myconcern and report in accordance with school procedures.

- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook which can be found on the school shared platform
- Notify the DSL/DDSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- When supporting pupils remotely, be mindful of additional safeguarding considerations
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their AUP at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/DDSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/DDSL know
- Receive regular updates from the DSL/DDSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE / RSHE Lead/s – Jessica Williams

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. This includes being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Address online safety and appropriate behaviour in an age-appropriate way that is relevant to pupils' lives.
- Work closely with the DSL/DDSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.

- Work closely with the Computing lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – Ella Heredge Thomas

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Review the computing curriculum, which covers the principles of online safety in school, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum, with support from the Head Teacher and Network Manager where necessary.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/DDSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context (https://www.gov.uk/government/organisations/uk-council-for-internet-safety)
- Work closely with the DSL/DDSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – Paul Moore

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for **pupils in the home on school given devices** and **remote-learning** procedures, rules and safeguards.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- Work closely with the designated safeguarding team and data protection officer to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems
- Support and advise on the implementation of ‘appropriate filtering and monitoring’ as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school’s online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school’s systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

Data Protection Officer (DPO) – Rina Begum

Key responsibilities:

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced ‘safeguarding’ as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children.”

- Work with the DSL, head teacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

LGfL TRUSTnet Nominated contacts – Paul Moore, Jessica Williams and Ella Heredge Thomas

Key responsibilities:

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL Team and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode,

internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.

- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL at gdpr.lgfl.net

Volunteers and contractors (including tutors employed by the DfE)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Treat home learning in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it

- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning and flag any concerns
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

External groups including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Education and curriculum

It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise

Whenever overseeing the use of technology in school or setting homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. Refer to saferesources.lgfl.net which provides updated theme-based resources, materials and signposting for teachers and parents.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding. General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff should be aware they may find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Specific Considerations:

Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying is treated like any other form of bullying and the school bullying policy should be followed. It is important not to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline elements.

The bullying policy can be found on the school website and shared platform

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

Sexual violence and harassment is now part of Keeping Children Safe in Education: Part 5 paragraphs 446-454.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL. Staff should work to foster a zero-tolerance culture. Christ Church CE Primary schools must take all forms of sexual violence and harassment seriously. We have a zero-tolerance approach to sexual violence and sexual harassment and it will not be tolerated. It should never be passed off as “banter”, “just having a laugh”, “a part of growing up” or “boys being boys”. Failure to do so can lead to a culture of unacceptable behaviour, an unsafe environment and in worst case scenarios a culture that normalises abuse, leading to children accepting it as normal and not coming forward to report it.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct in the school handbook.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Christ Church CE Primary School community. These are also governed by school Acceptable Use Policies.

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Christ Church CE Primary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net; there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.

Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information a **record of who they are sharing that information with and for what reason will be recorded. If they have taken a decision not to seek consent from the data subject and/or parent/carer that will also be recorded within the safeguarding file.**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found here. https://www.christchurchprimarybricklane.org/gdpr

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of USO-FX / Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to ensure appropriate filters and appropriate monitoring systems are in place to ensure children are not be able to access harmful or inappropriate material but at the same time be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Christ Church CE Primary School we have decided that Webscreen3 is appropriate because it allows the school to filter content appropriately.

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Pupils at this school use the PupilMail system from LGfL for all school emails
- Staff at this school use the Office365 system for all school emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email and Google Classrooms the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer/headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular

circumstances of the incident will determine whose remit this is) should be informed immediately.

- Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.
    - Internally, staff should use the school network, including when working from home when remote access is available via the Freedom2Roam system.
- Pupils are restricted to emailing within the school and cannot email external accounts
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the responsibility to updating the content of the website to Jo Gibney. The site is managed by Living and hosted by Siteground. Day-to-day updates will be delegated to Lusna Begum.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public-domain images that can be. Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

Cloud platforms

For online safety, basic rules of good password protocols. Expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud

- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Christ Church CE Primary School, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Christ Church CE Primary School's SM presence

Christ Church CE Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Ella Heredge Thomas is responsible for managing our Twitter account.

Staff, pupils' and parents' SM presence

Social media is a part of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and wh.

The school has an official Twitter account and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor. Staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, LDBS or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

School devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Year 6 Pupils** are allowed to bring mobile phones in for emergency use only. They are to be given in at the office when the children arrive at school and can be collected at the end of the day. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded

onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they must seek approval from a member of SLT and will be handled on a case-by-case basis. Alternatively, staff may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

- **Volunteers, contractors, governors** should leave their phones in their pockets and on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets, out of sight, when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network / internet access on school devices

- **Pupils/students** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
- **Home devices** are issued to some students. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked.
- **Volunteers, contractors, governors** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher, and staff authorised by them, have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Appendices

1. Safeguarding Incident log via MyConcern
2. Safeguarding and Child Protection Policy - www.christchurchprimarybricklane.org/policies
3. Behaviour Policy / Anti-Bullying Policy - www.christchurchprimarybricklane.org/policies
4. Staff Code of Conduct / Handbook – hard copy available from school office
5. Acceptable Use Policies (AUPs) for:
   - Pupils KS1 / KS2 – hard copy available from school office
   - Staff, Volunteers Governors & Contractors – hard copy available from school office
   - Parents – hard copy available from school office in pupil admissions form
6. Prevent Risk Assessment Template
7. Online-Safety Questions from the Governing Board (UKCIS)
8. Education for a Connected World cross-curricular digital resilience framework (UKCIS)
9. Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
10. Working together to safeguard children (DfE)
11. Searching, screening and confiscation advice (DfE)
12. Sexting guidance from UKCIS
    - Overview for all staff
    - Full guidance for school DSLs
13. Prevent Duty Guidance for Schools (DfE and Home Office documents)
14. Data protection and data security advice, procedures etc
15. Preventing and tackling bullying (DfE)
16. Cyber bullying: advice for headteachers and school staff (DfE) – find this at bullying.lgfl.net
17. RAG (red-amber-green) audits for statutory requirements of school websites