

Online Safety Policy

Agreed and Approved by the LGB

On
May 2022

CONTENTS

Document Control	2
Authorisation	2
Change History	2
Document References	2
Distribution List	2
Abbreviations	3
Policy	4

DOCUMENT CONTROL

Authorisation Authorised by: Local Governing Body Date: 9th March 2021 Change History

Editor	Comment	Date	Version
Jen Sinclair	Revised Draft	20/09/13	1.1
T Farrelly	Minor Amendments	20/09/13	1.2
Full Governing Bod	Agreed/approved	24/09/13	2.0
Claire Eastmond	Revised Draft	10/10/14	2.1
Claire Eastmond	Revised Draft	15/10/15	2.2
Claire Eastmond	Revised Draft	09/11/16	2.3
T Farrelly	Reviewed	10/11/16	2.4
Katie Flanagan	Revised Draft	29/10/17	2.5
Claire Eastmond	Reviewed	29/10/17	2.6
Local Governing Body	Agreed and Approved	24/4/19	3.0
Natasha Grant	Reviewed	7/5/19	3.1
Natasha Grant	Reviewed	19/2/21	3.2
Natasha Grant	Reviewed	24.4.22	3.3

Document References

#	Title	Date	Version
1	London Grid for Learning (LGfL) Acceptable Use Policy	16/06/11	1.0

Distribution List

Name	Date	Method
Trish Farrelly	November 2016	Email
All Staff	November 2016	By hand
School community	November 2016	MLE
Staff and School community	May 2019	Newsletter & Website
Staff and School community	March 2021	Newsletter & Website
Staff and School community	May 2022	Website

Abbreviations

Abbreviation	Meaning
Apps	Self-contained programs or pieces of software designed to fulfil a particular purpose.
DfE	Department for Education
LEA	Local Education Authority
LGfL	London Grid for Learning
MLE	Managed Learning Environment
URL	Uniform Resource Locator

COURTWOOD PRIMARY SCHOOL

ONLINE SAFETY POLICY

E-Safety covers issues relating to children, young people and adults when using the Internet, mobile phones, and other electronic communications technologies, both in and out of school. E-Safety provides education on risks and responsibilities of using technology and is part of the 'duty of care' which applies to everyone working with children. It is also about making sure that the school provides safeguards and raises awareness to enable users to control their own online experiences.

Courtwood Primary School is committed to supporting pupils in becoming knowledgeable around all aspects of the digital world and becoming good digital citizens whilst keeping them safe and teaching them how they can keep themselves safe in a continuously evolving technological world.

~~The impact of Covid-19 is at the forefront of our planning to support pupils. Periods of national lockdown has led to children being online more often and for longer/extended periods of time. We want to support pupils and their families to manage any additional pressures and/or anxieties such usage may have caused through a careful, nurturing and solution focused approach.~~

SCOPE

This policy applies to all members of the Courtwood Primary School community (including teaching and support staff, supply teachers and tutors engaged under the DFE National Tutoring Programme, governors, volunteers, contractors, 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 site.

INTRODUCTION

The purpose of this policy is to:

- Set out clear principles and expectations for all Courtwood 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)
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken.

ROLES AND RESPONSIBILITIES

PRINCIPAL & SENIOR LEADERSHIP TEAM (SLT)

The Principal has overall duty of care for ensuring the safety (including online safety) of members of the school community. The Principal and SLT are responsible for ensuring that staff receive suitable training to enable them to carry out their roles.

DESIGNATED SAFEGUARD LEADS (DSLs)

The DSLs will take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

They will remind staff of safeguarding concerns as part of the review of remote learning and will ensure the same principles and expectations for online safety and behaviour apply.

Teachers and Support Staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education
- Read, understood, and signed the staff acceptable use agreement.
- Have an up-to-date awareness of online safety matters and of the current school online safety policy and practices. Have an awareness and oversight of safeguarding provisions for **home-learning** and **remote-teaching technologies**
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- 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.
- 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 ageappropriateness of websites.
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the [20 Safeguarding Principles for Remote Lessons](#) infographic which applies to all online learning.
- Ensure pupils understand and follow the Online Safety Policy at home as well as at school.
- Manage pupil behaviour in line with the Behaviour Policy and Anti-Bullying Policy.
- 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.

BACKGROUND

The Education and Inspections Act 2006 empowers the Principal, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

HANDLING INCIDENTS

- The school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Any suspected online risk or infringement is reported to the Principal and Computing Co-ordinator that day.
- Any concern about staff misuse is always referred directly to the Principal, unless the concern is about the Principal in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

WHY IS INTERNET USE IMPORTANT?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business, and social interaction. The school has duty to provide students with quality Internet access as part of their learning experience.
- The Internet is the tool used to host Courtwood's learning and communication resource including Facebook and Twitter.

HOW DOES THE INTERNET BENEFIT EDUCATION?

Benefits of using the Internet in Education include:

- Access to software for teaching the computing curriculum.
- Enabling remote learning platforms, ensuring pupils can continue learning and access lessons remotely during periods of national lockdown and/or isolation.
- Access to worldwide educational resources including museums and art galleries.
- Inclusion in government initiatives such as the national Grid for Learning LGfL)
- Educational and cultural exchanges between pupils worldwide.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Develop more effective forms of interschool communication tools.
- Staff professional development through access to national developments, educational materials, and good curriculum practice.
- Communication with support services, professional associations and colleagues; improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the LEA and DfE.

HOW WILL INTERNET USE ENHANCE LEARNING?

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Pupils will use a variety of online software which will enable them to access the curriculum.

- Staff should guide pupils to use Apps and on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.
- Pupils will have access to a safe and secure learning environment through safe internet use at home.
- Pupils are able to access lessons remotely via Google Classroom during periods of national lockdown and/or isolation.
- Pupils are able to maintain daily contact with school adults and peers via Google Meet.

HOW WILL ONLINE SAFETY BE COMMUNICATED?

This school:

- Uses the Purple Mash Computing Scheme of Work to teach a range of skills and behaviours, appropriate to age and experience, covering online safety.
- Plans online carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- Ensure pupils only use school-approved systems and publish within appropriately secure / age appropriate environments.
- Makes online safety training available to teaching staff.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy.
- Provides online safety advice sessions for parents.

HOW WILL PUPILS LEARN TO EVALUATE INTERNET CONTENT?

- If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the Computing Co-ordinator. Pupils must inform the first available teacher if they find unsuitable sites. The instance will be recorded in the Internet Incident Log on the MLE.
- The school should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

HOW WILL EMAIL BE MANAGED?

- Pupils may only use approved LGFL email accounts on the MLE or Google Education email. Anonymous systems such as Hotmail are not allowed.
- Staff at Courtwood Primary School use email as set up by the Collegiate Trust for all school email.
- Emails are fully auditable, trackable, and managed by The Collegiate Trust 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.
- Email along with the chat functionality of Google Classroom are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used.

- Pupils are aware of their responsibility using email responsibly and sign a usage agreement referring to responsibilities and consequences.
- 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 are not to give out email user account to outside agencies/persons unless authorised by the class teacher.
- Pupils must immediately tell a teacher if they receive offensive email. The instance will be recorded in the Internet Incident Log.
- Pupils must not reveal details about themselves or others, such as address, telephone number or mobile number, or arrange to meet anyone in email or other electronic communication.
- Access in school to external personal email accounts is banned.
- Email sent to an external organisation should be written carefully and authorised by a teacher before sending.
- The forwarding of chain letters is banned.
- Pupils should be aware that school email will be monitored.
- Pupils and staff should be aware that all use is monitored, their emails may be read, and the same rules of appropriate behaviour apply at all times.

HOW WILL WEBSITE CONTENT BE MANAGED?

- The school website is a key public-facing information portal for the school community with a key reputational value.
- The point of contact on the website should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and parental permission will be obtained.
- Pupils' full names will not be used on the website when associated with photographs, or in any way which may be to the detriment of pupils.
- Pupils' photographs will immediately be removed from the school website upon request from parents, or another appropriate request.
- Pupils' work will be published with only name attached.
- The Principal will take overall editorial responsibility and ensure content is accurate and appropriate. The website should comply with the School's Guidelines for publications
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

SOCIAL MEDIA

- Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact 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 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 urge them to contact the school directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedures should be followed.
- Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), despite this the school is required on occasions to deal with issues arising on social media with pupils under the 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 must 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/students 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.
- 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.

HOW WILL THE SCHOOL TWITTER AND FACEBOOK ACCOUNTS BE MANAGED?

- The school Twitter and Facebook accounts will be managed by teaching staff only
- The school Twitter and Facebook accounts will be private accounts. This means the account holder can choose who to follow the account and any followers have to be approved by one of the account holders.
- As private accounts no other Twitter/Facebook user can 'retweet' or share a school tweet/post.
- The school Twitter and Facebook accounts will only tweet/post between the hours of 8am and 6pm between Monday and Friday. The only time tweets/posts outside of this time are for school events (e.g. football matches, residential trips, performances) or to share urgent school news (e.g. closers due to adverse weather).
- The school Twitter and Facebook accounts will only follow educationally link accounts. No personal accounts, unless they are educationally linked, will be followed. For example, a children's author.
- The school Twitter and Facebook accounts will not reply to any 'replies'. This is not the platform to discuss or debate school related issues.
- The school Twitter and Facebook accounts will only use children's first names when referencing children.
- The school Twitter and Facebook accounts will share positive messages about the school.
- The accounts may be used to share news and information during a school trip. The accounts will be managed by a senior teacher on a 3G connected phone for the period of the trip. Photos taken on the phone for the purpose of sharing on Twitter/Facebook will be deleted once they have been shared.
- *Individually targeted content* will not be posted e.g. "Well done Josh a better lesson today". Tweets/posts to a year group or class along the lines of "don't forget the..." are acceptable. Although always think about the most effective way to communicate important information.
- By endorsing Twitter/Facebook we may be encouraging children to use twitter so will reinforce online safety rules such as "Never tweet/post anything that would be potentially upsetting; make sure you know how to report to anything you find that disturbs you; be careful who you talk to they may not be all they appear; never meet anyone from twitter world without telling your parents." etc.

HOW WILL INTERNET ACCESS BE AUTHORISED?

- All staff and pupils will be granted Internet access.
- All members of staff need to have access to the online safety policy and rules for internet access.
- All staff agree to the Acceptable Use Policy

HOW WILL IPAD AND CHROMEBOOK USE BE MANAGED?

- Each class has iPads. All iPads across the school are linked so that all apps are the same on each of the iPads. All teacher iPads have the same passcode, and all pupil iPads have the same passcode. Children only know the pupil passcode and do not access to the teacher iPad without teacher permission.
- Teachers are responsible for checking the validity and appropriateness of any apps downloaded to their iPads and Chromebooks.
- Paid iPad apps will be managed by the Computing Co-ordinator, who will download teacher requests with the help of the IT support for the school.
- Teachers are responsible for monitoring the use of iPads and Chromebooks in their class.

HOW WILL THE USE OF MOBILE DEVICES BE MANAGED ?

Mobile devices refers to mobile phones, tablets and other mobile devices

- Personal mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- 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.
- All pupils' personal mobile devices will be handed into the school office should they be brought into school and collected at the end of the day.
- Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Principal should be sought (the Principal may choose to delegate this) and this should be done in the presence of a member staff.
- No images or videos should be taken on personal mobile devices.
- All visitors are requested to keep their phones on silent.
- The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- Staff mobile devices may be searched at any time as part of routine monitoring.

HOW WILL THE USE OF DIGITAL IMAGES AND VIDEO BE MANAGED?

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education and also taught to consider how to publish for a wide range of audiences.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. 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 are subject to bullying or abuse.

Page

HOW WILL THE RISKS BE ASSESSED?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the internal scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school has in place the LGfL filter service Syntetrix & Forensic Software to help regulate the safety of the internet for all the school community.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed regularly by the Principal and Computing Co-ordinator.
- The Principal and Computing Co-ordinator will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

HOW WILL FILTERING BE MANAGED?

- The school will work in partnership with Parents/Carers, The Collegiate Trust, the LEA, DfE and the Internet Service Provider to ensure that the systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet service provider via an internet incident log.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

HOW WILL THE POLICY BE INTRODUCED TO PUPILS?

- Pupils should be reminded of the internet and iPad rules. These should be printed as posters for the computer areas in the school.
- Rules for internet access will be posted on or near all computer systems.
- Pupils will be informed that internet use will be monitored.
- Instructions in responsibility and safe use should precede internet access through the school online safety program.
- Termly online safety assemblies.

HOW WILL STAFF BE CONSULTED?

- Staff should be aware that internet can be monitored and traced to the individual user. Discretion and professional conduct is required.
- Staff development in the safe and responsible internet use and on School Internet Policy will be provided as required.

HOW WILL COMPLAINTS REGARDING TECHNOLOGY USE BE HANDLED?

- Responsibility for handling incidents will be delegated to the Principal or computing coordinator.
- Any complaints about staff misuse must be referred to the Principal or computing coordinator.
- Any online safety problems with the children must be logged and reported to Principal or computing coordinator.

HOW WILL PARENTS' SUPPORT BE ENLISTED?

- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstration, practical sessions, and suggestions for safe internet use at home.
- The school website will promote safe internet use.