Online Safety Policy

Date: Autumn 2024

Review: Autumn 2027

Ferndale Primary School
School Policies

Ferndale Primary School
Online Safety Policy

Contents

	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	B Sansom
	Deputy Designated Safeguarding Leads / DSL Team Members	R Gillett, C Sykes, N Poole, A Cross, T Stanford, C Hall, S Robathan, B Finlan
	Link governor for safeguarding	[ ]
	Curriculum leads with relevance to online safeguarding and their role [e.g. PSHE/RSHE/RSE/Computing leads]	M Duggan – ICT lead T Edwards – PSHE / RSHE lead
	Network manager / other technical support	G Massey
	Date this policy was reviewed and by whom	[ ]
	Date of next review and by whom	[ ]

2. Introduction and Overview Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Ferndale Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Ferndale Primary School
- assist school staff working with children to work safely and responsibly withthe internet and other communication technologies and to monitor their ownstandards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying whichare cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary orlegal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adultswho work with Pupils.

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 leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks?

Online risk to children is classified according to the 4 C's: content, contact, conduct and commerce.

Content

- exposure to inappropriate content, including online pornography, ignoring ageratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Peer on peer protection

We recognise that children can abuse other children. This is referred to as peer on peer abuse and can take many forms that may be demonstrated through poor behaviour in the school setting; bullying (including cyber-bullying); sexual violenceand sexual harassment (online or via texts); sexting and initiating/hazing type violence and rituals. Part 5 of keeping children safe in education covers 'child-on-child sexual violence and sexual harassment'. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance.

Nationally, some of the latest trends of the past twelve months are outlined below:

Self-generative artificial intelligence has been a significant change, with children having often unfettered access to tools that generate text and images at home or in school. These tools represent a challenge in terms of accuracy when young people are genuinely looking for information.

The continued cost-of-living crisis has meant that children have spent more time online and therefore exposed to all manner of online harms as families have had to cut back on leisure activities and the public provision of free activities for young people has reduced further.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

Sanctions will be issued inline with this policy, alongside the Safeguarding Policy and relevant outside agencies may be informed. Support for the victim will reflect the circumstances of the incident, but could be offered internally through the school's own pastoral processes or through external agencies as a result on an early help assessment.

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred toas SGII (self-generated indecent images)
- Copyright, ensuring consideration for intellectual property and ownership –such as music and film.

Personal Devices

Pupils are prohibited from bringing personal devices into the classroom. Please refer to the mobile phone policy.

The Head teacher, Deputy head teacher and Assistant head teachers (SLT) are excluded from the above statement and therefore can use their personal devices insituations where school devices are not available to hand.

Staff must not take photographs of children on their own devices.

EYFS staff must also refer to Statutory Guidance for Mobile phones and school's acceptable use guidance.

Scope

This policy applies to all members of Ferndale Primary School community (including teaching, supply and support staff, 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.

Depending on their role, all members of the school community should read the relevant section in Annex A of this document that describes individual roles and responsibilities.

In 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues

Handling complaints:

- The school will take all reasonable precautions to maintain online safety; however, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions (See Behaviour Policy).
- Parents / Carers will be informed 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 concerning or breaks the law.
- Our designated safeguarding officers act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti- Bullying

Policy and Behaviour Policy. Complaints related to child protectionare dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The online safety policy is referenced from within other school policies: Child Protection policy, Anti-Bullying policy, Behaviour policy, PSHME policies.

- The school has an online safety coordinator who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The online safety policy has been written by the school online safety coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments tothe school online safety policy will be discussed in detail with all members ofteaching staff.

Bullying

Online bullying, including incidents that take place outside school or from home are treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

3. Education and Curriculum

Pupil online curriculum

This school has a clear, progressive online safety education programme as part ofthe Computing curriculum / wellbeing curriculum. This covers a range of skills andbehaviours appropriate to their age and experience. The school used Project EVOLVE and Google Internet Legends as resources to support the programme of study.

In order for children to achieve this they should…

- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understandthat this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web contentcan attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to recognise the dangers and issues surrounding online gaming/social media

including interacting with others online, interacting through VOIP (Voice Over IP [voice communications]) and age restrictions.

- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files – without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know howto seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seekhelp if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

The school should:

- Plan Internet use carefully to ensure that it is age-appropriate and supportsthe learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities
- Ensure staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that when copying materials from the web, staff and pupils understandissues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- Ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks inpop-ups; buying on-line; on-line gaming / gambling.
- Annual reviews of curriculum plans / schemes of work are used as an opportunity to follow key areas such as self – image and identity, online relationships, online reputation, online bullying, managing online information, privacy and security and copyright and ownership.

Staff and governor training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education programme, through annual updates andannual staff meetings.
- 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 safeguarding policy and the school's Acceptable Use Policies.
- Support staff training on identifying phishing or harmful emails by using phishing

attack simulations.

Parent awareness

This school:

Runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online behaviour are made clear
- Information leaflets; in school newsletters; on the school web site;
- suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.

4. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign beforebeing given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practicewhen using digital technologies out of school and realise that the school'sOnline Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber- bullying

Staff

- are responsible for reading the school's online safety policy and using theschool ICT systems accordingly, including the use of mobile phones, andhand held devices.

Pupils/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what

sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions (See Behaviour Policy), though the attitudes and behaviour of users are generally positive and there israrely a need to apply sanctions.
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- monitoring and reporting of online safety incidents takes place and contributeto developments in policy and practice in online safety within the school. Therecords are reviewed / audited and reported to the school's senior leaders, Governors.
- Parents / carers are specifically informed of online safety incidents involvingyoung people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- SENSO is used to monitor computers. Please refer to the filtering and monitoring policy.

5. Managing the ICT infrastructure

Internet access, security (virus protection)

This school:

- Has the educational filtered secure broadband connectivity through SIPS (Sandwell Inspired Partnership) Broadband Services and uses the SandwellNet Sweeper filtering system which blocks sites that fall into categories suchas pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of anti-virus software and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or Sandwell approved systems such as 'MOVEit' to send personal data over the Internet and uses encrypted devices or secure remoteaccess where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are partof an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Video conferencing such as Microsoft teams and zoom has been enabled for staff.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable,and

uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- Ensures all staff and Pupils have signed an acceptable use agreement formand understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct Pupils to age / subject appropriate web sites. Google Safe Search is always on.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google imagesearch;
- Informs all users that Internet use is monitored;
- Informs staff and Pupils that that they must report any failure of the filtering systems directly to the [Online safety Co-ordinator and Network Manager]. Our system administrator(s) logs or escalates as appropriate to the Technicalservice provider or Sandwell Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use'are and what sanctions result from misuse – through staff meetings
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school:

- Uses individual log-ins for all users
- Uses guest wifi access for external or short-term visitors
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Ensures the Systems Administrator / network manager is up-to-date with Sandwell services and policies / requires the Technical Support Provider to beup-to-date with Sandwell services and policies;
- Storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety policy. Following this, they are set-up with Internet, email access andnetwork access. We provide a different username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- Pupils use logins and their internet activity can be monitored by SENSO.
- We use the Office365 Learning Platform system with individual username and passwords.
- Makes clear that no one should log on as another user and makes clear thatpupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damagefiles or the network;
- Google classrooms is used for remote learning with individual usernames and passwords.

- Requires all users to always log off when they have finished working or areleaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-offand then log-on again as themselves. Computers left on can be remotely logged off or locked.
- Makes clear that all equipment that goes home has the anti-virus and spyware software maintained up-to-dateand the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significantpersonal use".
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnelsystem etc.
- Does not allow any outside Agencies to access our network remotely exceptwhere there is a clear professional need and then access is restricted and isonly through approved systems;
    - e.g. technical support or MIS Support, our Attendance and Prosecution Service accessing attendance data on specific children and other LA approved partners
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password.
- Has a clear disaster recovery system in place for critical data that includes asecure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through secure file exchange (MOVEit);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of ournetwork;
- Our wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safetyand security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it whereothers can find it;
- All staff have their own unique username and private passwords to accessschool systems. Staff are responsible for keeping their password private.
- We require staff to use strong passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, periodically
- 2FA (two-factor authentication is used where appropriate

.

E-mail

- Provides staff with an Office 365 email account for their professional use, andmakes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example office@ferndale.sandwell.sch.uk
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary, to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of Office365 provided technologies to help protect users and systems in the school, including desktop anti-virus productSophos. Finally, and in support of these, LGFL filtering monitors and protects our Internet access to the World Wide Web.

Staff:

- Staff can only use the school's Office365 e-mail systems on the schoolsystem for professional use.
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. We use secure, LA /DfE approved systems.
- All staff sign our AUP to say they have read and understood the online safetyrules, including e-mail and we explain how any inappropriate use will be dealtwith.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity orstatus;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, which is admin@ferndale.sch.ukHome information or individual e-mail identities will not be published

- Photographs published on the web do not have full names attached; and willhave parental consent.
- We do not use pupils' names when saving images in the file names or in thetags when publishing to the school website;

Social networking

Social media and social networking sites plan an important role in the lives of many people. We recognise that sites bring risks, but equally there are many benefits to be reaped.

There are four key areas:
A. The use of social networking sites by pupils within school
B. Use of social networking by staff in a personal capacity
C. Comments posted by parents/carers
D. Dealing with incidents of online bullying

Please refer to the social network policy for clarity to the way in which social media / mobile phones are to be used by pupils, governors, visitors, parents and school staff at Ferndale.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Policeas part of a criminal investigation.

6. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Business Manager is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection mayhave been compromised.
- All staff are DBS checked and records are held in one central record MIS –SIMS.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - Staff
  - Reception children and parents

- This makes clear staffs' responsibilities with regard to data security, passwords and access.

Technical Solutions

- We require staff to log-out of systems when leaving their computer
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools. We use the MOVEit system to transfer admissions data.
- We use MOVEit to transfer other data to schools across the Borough, such as references, reports of children.

- All servers are in lockable locations and managed by DBS-checked staff.

Cybersecurity

The school works to the DFE guidelines – ‘meeting digital and technology standards in schools’ by:

- Ongoing training and learning on cyber awareness for children and staff
- Control and secure user accounts and access privileges
- Reporting any cyber attacks
- Secure technology and data with anti-malware and firewalls
- Use of LGFL guidance and resources for cyber security
- Conduct cyber risk assessments annually.

Filtering and Monitoring

Please refer to the filtering and monitoring policy. Ferndale follows the DFE filtering and monitoring standards, which require the school to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

According to the DfE standards, “a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

7. Equipment and Digital Content – See also use of Mobile phones (Staff Handbook)

Personal mobile phones and mobile devices

(See policy for the use of mobile phones)

Pupils’ use of personal devices

- The School policy is that pupils do not bring personal devices in to school. If amobile device is found, they will be placed in a secure location and can be collected by an adult at the end of the school day.
- The School accepts that there may be particular circumstances in which aparent wishes their child to have a mobile phone for their own safety. Thatmobile phone will be kept in a secure location in the school office.
- Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff handheld devices are not permitted to be used to take images / videos oraudio recording in school.
- When using personal devices to make welfare calls to families, staff mustensure that they hide their caller ID (by inputting 141) before they dial thenumber.
- Staff will be issued with a school phone where contact with Pupils, parents orcarers is required.
- Mobile Phones and personally-owned devices will be switched off or switchedto 'silent' mode.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- The exemptions to all of the above clauses are the Head Teacher, Deputy Head Teacher and Assistant Head Teachers (SLT), who should, whenever possible, be in possession of their mobile phones so that they may act and make appropriate contacts in the case of an emergency. They are excludedfrom the above statement and therefore can use their personal devices in situations where school devices are not available to hand and agree to remove pictures as soon as possible.
- If a member of staff breaches the school policy then disciplinary action maybe taken.

Digital images and video in this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the online consent 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;
- Staff sign the school's Acceptable Use Policy and this includes a clause onthe use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, inthe prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroupsunless

there is a specific approved educational purpose;

- 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 tomaintain privacy settings so as not to make personal information public.

Appendix – Roles

Role	Key Responsibilities
Headteacher	• Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding • Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance • Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements • Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE. • 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 • Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • Ensure the school website meets statutory requirements • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service,which complies with current statutory requirements e.g. Sandwell • To be responsible for ensuring that staff receive suitable training to carry out their e- safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online safety incident. • To ensure that there is a system in place to monitor and support staffwho carry out internal online safety procedures
DSL	• To take overall responsibility for online safety provision • Ensure "An effective whole school approach to online safety as per KCSIE • Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised • Ensure ALL staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated. • Take day-to-day responsibility for safeguarding 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 closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)

	• Work with the headteacher, DPO and governors to ensure a 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 • Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors • Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
E-Safety Co-ordinators & Designated Safeguarding leaders for each building (Deputy and Assistant Headteachers)	• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents • promotes an awareness and commitment to online safety throughoutthe school community • ensures that online safety education is embedded across the curriculum • liaises with school ICT technical staff • To communicate regularly with SLT and the designated online safety Governor / committee to discuss current issues, review incident logsand filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that any online safety incidents are recorded on CPOMS • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: o sharing of personal data o access to illegal / inappropriate materials o inappropriate on-line contact with adults / strangers o potential or actual incidents of grooming o cyber-bullying and use of social media
Governors / Led by safeguarding link governor	• To ensure that the school follows all current online safety advice tokeep the children and staff safe • To approve the Online safety Policy and review the effectiveness ofthe policy. • To support the school in encouraging parents and the wider community to become engaged in online safety activities • Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated • Regular review with the Online safety Co-ordinator / Officer (including online safety incident logs, filtering / change control logs)

	• Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
Computing Curriculum Leader / PSHE – RSHE leader	• To oversee the delivery of the online safety element of the computing curriculum and PSHE-RSHE curriculum • To liaise with the online safety coordinator regularly • Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within computing and PSHE / RSHE. • 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
Network Manager / IT technician	• To report any online safety related issues that arises, to the online-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • To 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 • That the use of the network / Learning Platform/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online safety Co-ordinator / IT Technician /Head teacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures • To ensure that all data held on pupils on the Learning Platform is adequately protected • Work with the Headteacher to ensure the school website meets statutory DfE requirements
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place • Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the taking / use of images and on cyber- bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
Parents/carers	• to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to take care and use any equipment loaned from the school to support online learning appropriately. Only to use approved websites and services.