RICHMOND HILL SCHOOL
ONLINE SAFETY POLICY & PROCEDURES

Head teacher	**Rachel Blair**
Designated Safeguarding Lead (DSL)	**Rachel Blair**
Online Safety / Safeguarding Link Governor	**Amanda Coates**
PSHE / RSHE lead	**Charlotte Bonnar**
Network Manager / other technical support	**Alison Cattanach**

Approved by[1]			
Name:	**Rachel Blair**		
Position:	**Headteacher**		
Signed:			
Date:	9.10.26	**Version No:**	11
Review date[2]:	9.10.27		

[1] The Governing Body are free to delegate approval of this document to a sub-committee , an individual Governor, or the Head Teacher.
[2] Governors free to determine review period. Recommended annually.

REVIEW SHEET

Each entry in the table below summarises the changes to this Policy and procedures made since the last review (if any).

Version Number	Version Description	Date of Revision/Review
1	Original. Complete rewrite to take into account current national guidance on Online Safety	Nov 2019
2	Updated in line with Keeping Children Safe in Education 2020. No legal or significant policy changes just updates to link document mentions to the latest versions of them online (not highlighted). Minor policy addition in Section 3 to draw attention to policy or procedure addendums staff and others must be aware of (usually Covid-19 related). Minor policy clarification in Section 9.1 (BYOD procedures) just to specifically reference wearable technologies and the broadcasting of location data (highlighted).	Sept 2020
3	Updated to include additional information on sharing nude and semi-nude images and online challenges and hoaxes.	Mar 2021
4	Updated in light of statutory DfE guidance 'Keeping Children Safe in Education' Sept 2021 which newly references schools having an online safety policy and what it should contain, the 4Cs, and the continuing DfE expectation that all schools responsible for the provision of compulsory schooling (including independent schools with pupils funded by the taxpayer i.e. children looked after or children from military families attending boarding schools) will provide remote education and do it safely. Minor updates to appendices to reflect language/KCSiE updates.	Sept 2021
5	Updated in line with statutory DfE guidance 'Keeping Children Safe in Education' Sept 2022. Changed BYOD into section 9.2 to make it easier to find and reference (no content changes). Significant chunks of the Remote Learning section removed and replaced with links to government guides. Appendices removed and replaced with links to separate documents that are easier to use, update and distribute. Other links all checked as correct.	Sept 2022
6	Updated in line with KCSiE 2023 (filtering and monitoring) and to various links	Sept 2023
7	Removed the link to the KAHSC filtering and monitoring guidance which now forms Appendix A as an additional document and provides specific detail on how the school will manage filtering and monitoring of the technology used and of school-owned devices. Schools should complete the Appendix and publish with the Policy and procedures.	Nov 2023
8	Minor updates with links to DfE guidance for schools on creating a Mobile Phone Policy/procedure for pupils.	Feb 2024
9	Updated in line with revised DfE Digital and technology standards in schools and Generative artificial intelligence (AI) in education.	Sept 2024
10	Minor changes in line with KCSiE 2025 and for clarity. Updated with references to DFE guidance on Artificial Intelligence (AI) and updated broken links. Updated links to LA Safeguarding Children Partnership websites and change of name of the former Cumberland Safeguarding Hub (09/09).	Sept 2025
11	Updated to include advice from UKCIS on 'Protecting your setting's images from AI manipulation and abuse' and KCSiE 2026 .	Sept 2026

CONTENTS

POLICY 1
1. Background/Rationale 1
2. Definitions 1
3. Associated School Policies and procedures 2
4. Communication/Monitoring/Review of this Policy and procedures 2
5. Scope of the Policy 2
PROCEDURES 3
1. Roles and Responsibilities 3
1.1 Governors 3
1.2 Head teacher/DSL 4
1.3 All Staff 6
1.4 PSHE/RSHE Lead(s) 6
1.5 Computing/Subject Lead(s) 7
1.6 Network Manager/Technical staff 7
1.7 Data Protection Officer (DPO) 8
1.8 Volunteers and contractors 8
1.9 Pupils 8
1.10 Parents 9
2. Teaching and Learning 9
2.1 How internet use enhances learning 10
2.2 Pupils with additional needs 11
2.3 Remote Education 11
3. Handling online safety concerns and incidents 11
3.1 Sharing nudes and/or semi-nudes 12
3.2 Upskirting 13
3.3 Cyberbullying 13
3.4 Harmful online challenges or hoaxes 14
3.5 Harmful sexual behaviour, sexual violence and harassment 15
3.6 Misuse of school technology (devices, systems, networks, or platforms) 15
3.7 Social media incidents 15
4. Data protection and data security 16
4.1 Maintaining Information Systems Security 16
4.2 Password Security 17
5. Electronic Communications 18
5.1 Managing Email 18
5.2 Emailing personal, sensitive, confidential, or classified information 19
5.3 Zombie accounts 19
6. School Website 19
7. Use of digital and video images 20
8. Cloud Platforms 21
9. Social Media 21

9.1 Managing social networking, social media, and personal publishing sites 21
9.2 Personal devices and bring your own device (BYOD) procedures 23
10. Generative Artificial Intelligence 25
11. Managing filtering and monitoring 26
12. Webcams and Surveillance Camera Systems (incl. CCTV) 26
13. Managing emerging technologies 27
14. Cyber security and resilience 27
15. Policy Decisions 28
15.1 Authorising internet access 28
15.2 Assessing risks 28
15.3 Responding to incidents of concern 28
16. Communicating Policy and procedures 29
16.1 Introducing the Policy and procedures to Pupils 29
16.2 Discussing the Policy and procedures with Staff 29
16.3 Enlisting Parents' Support 30
17. Complaints 30
Richmond Hill School - Online Safety - Filtering and Monitoring Arrangements 1
1. Introduction 1
2. DfE Filtering and monitoring standards 2
3. Blocking harmful and inappropriate content 3
4. Filtering 4
5. Monitoring 5
6. Review of filtering and monitoring 6
7. Reporting safeguarding and technical concerns 8
8. Filtering and monitoring resource list / sources of further information 8

Appendix A – School specific information on managing filtering and monitoring of school-owned devices

Online Safety – links to various useful websites

Please note – Links below are to documents available from either the KAHub or external websites and are for school use only. Not all links will be relevant to your setting, please remove links prior to publishing.

360° safe - Online safety self-review tool for schools
Sample UKSIC EYFS, Primary and Special School Online Safety Posters (ages 3-6) (ages 7-11)
KAHSC Model EYFS, Primary & Special School pupil/parent Acceptable Use Agreement
KAHSC Model Staff/Volunteer Acceptable Use Agreement
KAHSC Model Governor Acceptable Use Agreement
KAHSC Response to an online safety incident or concern flowchart
KAHSC School specific filtering and monitoring checks record/log

POLICY

11. Background/Rationale

New technologies have become integral to the lives of children in society, both in and outside school.

The Internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity, and increase awareness of context to promote effective learning. Children have an entitlement to safe internet access.

The requirement to ensure that children can use online and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. The school Online Safety Policy and procedures will help to ensure safe and appropriate use, and the development and implementation will involve all stakeholders in a child's education from the Head teacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put children at risk in and outside of school. Some of the dangers they may face include:

- access to illegal, harmful, or inappropriate images or other content;
- unauthorised access to/loss of/sharing of personal information;
- the risk of being subject to grooming by those with whom they make contact on the internet;
- the risk of being targeted by extremists in order to promote and encourage radicalisation;
- the risk of being targeted by those involved in child sexual, criminal and financial exploitation;
- the making, sharing and/or distribution of images and/or other media without an individual's consent or knowledge;
- being drawn into taking part in unsuitable online challenges and/or hoaxes;
- inappropriate communication/contact with others, including strangers;
- cyberbullying (including prejudice-based and discriminatory bullying);
- access to gambling/gaming sites;
- access to unsuitable video/internet games;
- an inability to evaluate the quality, accuracy, and relevance of information on the Internet;
- plagiarism and copyright infringement;
- illegal downloading of music or video files;
- the potential for excessive use which may impact on the social and emotional development and learning of the child.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy and procedures is used in conjunction with other school Policies and procedures including the Child Protection, Data Protection and Behaviour.

As with all other risks, it is impossible to eliminate online risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

This school must demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The Online Safety Policy and procedures that follows explains how we intend to do this, while also addressing wider educational issues to help children (and their families) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal, and recreational use.

12. Definitions

For the purposes of this document a child, young person, pupil, or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

Wherever the term 'parent' is used this includes any person with parental authority over the child concerned e.g. carers, legal guardians etc.

Wherever the term 'Head teacher' is used this also refers to any Manager with the equivalent responsibility for children.

Wherever the term 'school' is used this will usually include wraparound care provided by a setting such as breakfast and after school clubs.

13. Associated School Policies and procedures

This Policy should be read in conjunction with the following school Policies/procedures and, where they exist, addendums to those Policies and procedures:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Data Protection Policy including procedures for surveillance systems (e.g. CCTV)
- Health and Safety Policy and procedures
- Behaviour Policy and procedures
- Use of images procedures
- Whistleblowing procedures
- Code of Conduct for staff and other adults
- Voluntary Home-School Agreement

14. Communication/Monitoring/Review of this Policy and procedures

This Policy and procedures will be communicated to staff, pupils, and the wider community by:

- posting it on the school website/Learning Platform/shared staff drive
- making a paper copy available on request from the school office and for staff
- discussing school policy and procedures during induction with new staff and other relevant adults including (where relevant) the staff Acceptable Use Agreement
- discussing Acceptable Use Agreements with pupils at the start of each year
- issuing Acceptable Use Agreements to external users of school systems (e.g. Governors) usually on first entry to the school
- holding signed Acceptable Use Agreements in pupil and personnel files

The Online Safety Policy is also referenced in other school Policies and procedures as outlined above.

15. Scope of the Policy

This Policy and procedures applies to all members of the School community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of our ICT systems, both in and out of school.

The Education and Inspections Act 2006 reasonably empowers Head teachers to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour, such as cyberbullying (including prejudice-based and discriminatory bullying), or other online safety related incidents covered by this Policy and procedures, which may take place out of school, but is linked to membership of the school. The Education Act 2011 increased these powers in relation to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken in relation to issues covered by the published Behaviour Policy and procedures.

The school will deal with adverse incidents in line with our Behaviour Policy and procedures (which includes anti-bullying procedures) and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

PROCEDURES

11. Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

1.1 Governors

The role of the Governors (Online safety Governor/Digital link Governor) is to:

- ensure a member of the Governing Body is elected to the role of Online Safety/Digital link Governor who should then lead on relevant governance requirements below;
- ensure an appropriate senior member of staff from the School Leadership Team (SLT) is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety and an understanding of the filtering and monitoring systems and processes in place) with the appropriate status, authority, time, funding, training, resources, and support. The DSL or an alternative member of SLT should be given the role of Digital technology lead;
- ensure an effective digital technology strategy is in place which is monitored and reviewed annually (see DfE Digital leadership and governance standard);
- ensure other roles and responsibilities are appropriately allocated to staff and third parties, e.g. external service providers in order to meet the DfE Digital and technology standards;
- ensure that systems are in place to meet the requirements of the DfE Cyber security standards. Schools must have a Cyber security and resilience strategy in place which is supported by an appropriate Cyber Response Plan;
- ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures;
- approve the Online Safety Policy and procedures, reviewing its effectiveness e.g. through Governors or a Sub-committee receiving regular information about online safety incidents, monitoring reports and making use of the UK Council for Internet Safety (UKCIS) guide Online safety in schools and colleges: Questions from the Governing Board;
- ensure that appropriate filters and monitoring systems are in place, but also consider how 'over-blocking' may lead to unreasonable restrictions on what pupils can be taught in relation to online teaching and safeguarding;
- ensure that the SLT and **all** staff have an awareness and understanding of the procedures and processes in place to manage filtering and monitoring and how to escalate concerns when identified;
- ensure all Governors receive appropriate training on online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring in relation to school owned IT devices. LGfL offer a range of free online courses/webinars for Governors;
- ensure that the school follows all current online safety advice to keep both pupils and staff safe;
- support the school in encouraging parents and the wider community to become engaged in online safety activities;
- have regular reviews with the Head Teacher and incorporate online safety into standing discussions of safeguarding at Governor meetings (including incident logs, adverse monitoring reports, change control logs etc.)
- work with the Data Protection Officer (DPO), DSL and Head teacher to ensure a UK GDPR compliant framework for storing data, helping to ensure that child protection is always at the forefront and data protection processes support careful and legal sharing of information;
- check that school is making good use of information and support (Annex A – Further information), which forms part of Keeping Children Safe in Education (KCSiE);
- ensure that all staff undertake regular updated safeguarding training, including online safety training, in line with advice from the Cumberland Safeguarding Children's Partnership (SCP), and that it is integrated, aligned, and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning;

- recognise that a one size fits all educational approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed;
- ensure pupils are taught how to keep themselves safe, including online as part of providing a broad and balanced curriculum with clear procedures on the use of mobile technology.

1.2 Head teacher/DSL

The Head teacher has overall responsibility for online safety provision.

The Head teacher will:

- take overall responsibility for data and data security;
- foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding;
- ensure that Policies and procedures are followed by all staff and other adults working paid or unpaid in the school;
- undertake training in offline and online safety, in accordance with statutory guidance and relevant Local Safeguarding Partnership recommendations;
- take responsibility for liaising with the Governors in order to achieve their obligations in meeting the DfE digital and technology standards, particularly as they relate to cyber security and filtering and monitoring and ensuring the Governors are regularly updated on progress towards the standards;
- ensure that online safety is appropriately monitored and reviewed by undertaking an annual review of the school's approach to online safety, supported by an annual review of the risk assessment that considers and reflects the risks the children face. We will use appropriate tools for this purpose such as the self-review tool 360° safe or LGfL online safety audit.
- take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO and Governors to ensure a Data Protection Act 2018 (DPA) compliant framework for storing data, but helping to ensure that child protection is always the first priority, 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, the use of generative Artificial Intelligence (AI) 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 on induction to carry out their child protection and online safety roles (which should include the procedures and processes in place to manage filtering and monitoring, the safe use of generative Artificial Intelligence (AI) and how to escalate concerns when identified). UKCIS have published an Online Safety Audit Tool which helps mentors of trainee teachers and early career teachers induct mentees and provide ongoing support, development and monitoring;
- understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident involving a pupil or an incident which results in an allegation against a member of staff or other adult (see flowchart for dealing with online safety incidents);
- encourage parents to provide age-appropriate supervision for children in their care using the internet including by the use of internet filters which should be used to block malicious websites (usually free but often need turned on. Information for parents will be regularly updated and published on the school website and via newsletters and other publications.
- ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including the risk of children being radicalised;
- take responsibility for formulating the school's Cyber security resilience strategy and Cyber response plan in liaison with the Online Safety Governor and other third party providers;
- ensure the school website meets statutory requirements (see KAHSC guidance on statutory and desirable website features and content for maintained or academy schools).
- have strategic oversight of all digital technology and how it fits with the school development plan;
- create and manage the digital technology strategy led by the needs of staff and pupils, not the

technology itself;

- help all staff to embed digital technology that meets staff and pupil needs;
- take lead responsibility for safeguarding and child protection (including online safety, the safe use of generative AI and understanding the filtering and monitoring systems and processes in place);
- be the first point of contact for any concerns the wider staff and other adults working in the school may have in relation to child protection and online safety harmful behaviour e.g. sharing nudes and/or semi-nudes and online challenges or hoaxes and refer to the UKCIS guidance Sharing nudes and semi-nudes: how to respond to an incident and the DfE Guidance Harmful online challenges and online hoaxes;
- ensure an effective digital technology strategy is in place that empowers the school to protect and educate the whole school community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate;
- source innovative ways to promote an awareness and commitment to online safety throughout the school community with strong focus on parents, who are often appreciative of school support in this area, but also including 'hard-to-reach' parents;
- have an understanding of the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school and to support other adults in doing so;
- ensure that online safety education is embedded in line with DfE guidance Teaching Online Safety in schools across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World' and the ProjectEVOLVE - Education for a Connected World Resources) and beyond, in the wider school community;
- work with the Data Protection Officer, Governors, and the school IT technical staff to ensure a DPA compliant framework for storing data, helping to ensure that child protection is always at the fore and data protection processes support careful and legal sharing of information;
- keep up to date with the latest local and national trends in online safety;
- review and update this Policy and procedures, other online safety documents (e.g. Acceptable Use Agreements) and the strategy on which they are based (in line with Policies and procedures for behaviour and child protection) and submit for review on a regular basis to the Governors;
- liaise with school technical, pastoral, and support staff as appropriate;
- communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs;
- ensure that 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 in the same way as any other child protection incident;
- oversee and discuss 'appropriate filtering and monitoring' with Governors in order to meet the DfE Filtering and monitoring standards (both physical and technical) and ensure staff are aware of its necessity;
- ensure the DfE guidance on child on child harmful sexual behaviour (HSB), sexual harassment and sexual violence (particularly online) (Part five - KCSiE) is followed throughout the school and that staff adopt a zero-tolerance approach to this as well as to bullying (in all its forms) generally;
- facilitate training and advice for staff and others working in the school to ensure that:
  - all staff who work directly with children must read and understand KCSiE Part one. The DSL, Head teacher, Safeguarding Governor and other members of the SLT must read and understand the whole of KCSiE;
  - knowledge of risks and opportunities is cascaded throughout the organisation.
- be aware of emerging online safety issues and legislation, and of the potential for serious child protection issues to arise from:
  - sharing of personal data;
  - the use of Generative Artificial Intelligence (AI);
  - access to illegal/inappropriate materials;
  - inappropriate online contact with adults/strangers;
  - potential or actual incidents of grooming;
  - cyberbullying and the use of social media.

1.3 All Staff

It is the responsibility of all staff to:

- understand that online safety is a core part of safeguarding; as such it is part of everyone's role. Never think that 'someone else will pick it up';
- know who the Designated Safeguarding Lead and Digital Technology Lead are;
- read and understand Part one of KCSiE;
- read, understand, and help promote the school's Online Safety Policy and procedures in conjunction with the Child Protection and other related school Policies and procedures;
- read, sign, and follow the school Staff Acceptable Use Agreement and staff Code of Conduct;
- be aware of online safety issues related to the use of mobile technology e.g. phones, cameras, wearable technology such as smart watches and meta glasses and other hand-held devices and follow school procedures in relation to these devices.
- ensure the security of their username and password for the school system, not allow other users to access the systems using their log on details and immediately report any suspicion or evidence that there has been a breach of security. Passwords will be changed on a regular basis and at least every 6 months;
- should understand (via training and other means) the different roles and responsibilities for the filtering and monitoring of online systems and expectations of them in their role, including for their own online activities on any device using the school network or on school-owned devices using any network;
- record online safety incidents in the same way as any child protection incident and report incidents to the DSL/DTL in accordance with school procedures;
- notify the DSL/DTL if policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon;
- 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 (devices, the Internet, new technology such as generative AI, etc.) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (check what appropriate filtering and monitoring processes are in place);
- carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data laws;
- prepare and check all online source and resources before using in the classroom;
- encourage pupils to follow their Acceptable Use Agreement, regularly remind them about it and enforce school sanctions where there is a breach of the Agreement;
- notify the DSL of new trends and issues before they become a problem;
- take a zero-tolerance approach to signs, reports and concerns of harmful sexual behaviour, child on child sexual harassment and sexual violence offline or online, including those occurring outside of the school premises and report any concerns to the DSL as soon as possible;
- receive and act upon regular updates from the DSL and have a healthy curiosity for online safety 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 the professional reputation of all staff;
- ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts.

1.4 PSHE/RSHE Lead(s)

Responsibilities of PSHE/RSHE Leads include:

- all as listed in the 'all staff' section above;

- ensuring that consent, mental wellbeing, healthy relationships and staying safe online is embedded into the PSHE/Relationships education, relationships, and sex education (RSE) and health education curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of the pupils' online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives (KCSiE);
- complementing the computing curriculum which covers the principles of online safety at all key stages, 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 the pupil has concerns about content or contact on the Internet or other online technologies;
- working closely with the DSL/DTL and all other staff to ensure an understanding of the issues, approaches, and messages within PSHE/RSHE.

1.5 Computing/Subject Lead(s)

Responsibilities of the Computing Lead include:

- all as listed in the 'all staff' section above;
- the overseeing delivery of the online safety element of the Computing curriculum in accordance with the national curriculum;
- working closely with the DSL and all other staff to ensure an understanding of the issues, approaches, and messages within Computing;
- collaboration with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with Acceptable Use Agreements.

1.6 Network Manager/Technical staff

Responsibilities of the Network Manager/ICT Technician include:

- all as listed in the 'all staff' section above;
- supporting Governors and SLT in achieving the DfE digital and technology standards;
- supporting SLT in the formulation of a Cyber Security resilience strategy and appropriate Cyber response plan as outlined in the DfE Cyber security standards;
- reporting any online safety related issues that arise through external monitoring reports, to the DSL/DTL in the first instance;
- keeping up to date with the school's Online safety Policy and technical information to effectively carryout their online safety role and to inform and update others as relevant;
- working closely with the DSL/DPO to ensure that school systems and networks reflect school Policy;
- ensuring that the above stakeholders understand the terms of existing services and how any changes to these systems (especially in terms of access to personal and sensitive records/data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.) might affect the system functions and safety online;
- supporting and providing advice on the implementation of 'appropriate filtering and monitoring' in order to meet the school's obligations outlined in the DfE Filtering and Monitoring standards;
- ensuring that users may only access the school's networks through an authorised and properly enforced password protection procedures, in which passwords are regularly changed;
- ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack e.g. keeping virus protection up to date;
- ensuring that access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
- monitoring the use of the network/Virtual Learning Environment (VLE)/remote access/email and social media presence and that any misuse/attempted misuse is reported to the DSL in line with school Policy;
- ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a cyber-attack or other disaster and to complement the business continuity process and cyber response plan;

- maintaining up-to-date documentation of the school's online security and technical procedures;
- working with the Head teacher to ensure the school website meets statutory DfE requirements;
- reporting online safety issues that come to their attention in line with school Policy.

1.7 Data Protection Officer (DPO)

The DPO will be familiar with references to the relationship between data protection and safeguarding in key DfE documents 'KCSiE' and 'Data protection: a toolkit for schools'.

The Data Protection Act 2018 and UK GDPR **do not** prevent, or limit, the sharing of information for the purposes of keeping children safe and promoting their welfare. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with DPA 2018. Legal and secure information sharing between schools, Cumberland Children Advice and Support Service (CASS) and other local agencies is essential for keeping children safe and ensuring they get the support they need. 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 the need to safeguard and promote the welfare of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

Other responsibilities of the DPO include:

- working with the DSL, Head teacher and Governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above;
- ensuring that all access to safeguarding data is limited as appropriate, monitored, and audited.

1.8 Volunteers and contractors

The key responsibilities of volunteers and contractors are to:

- read, understand, sign, and adhere to any Acceptable Use Agreement issued by the school;
- report any concerns, no matter how small, to the DSL/DTL without delay;
- maintain an awareness of current online safety issues and guidance;
- model safe, responsible, and professional behaviours in their own use of technology.

1.9 Pupils

Taking into account their age and level of understanding, the key responsibilities of pupils are to:

- use the school ICT systems in accordance with the age-appropriate Pupil Acceptable Use Agreement – see links on contents page, which they and/or their parents will be expected to sign before being given access to school systems.
- ensure the security of their username and password for the school system, not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- understand the importance of reporting abuse, misuse or access to inappropriate materials including those involving hoaxes and on-line challenges and know how to do so;
- know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- 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 agreements cover their actions out of school, including on social media;
- know and understand school procedures on the use of mobile phones, digital cameras, and other digital devices (see 9.2 below);
- know and understand school procedures on the taking/use of images and on cyberbullying/making and sharing nudes and/or semi-nudes, including where generated by AI;
- understand that the school is able to, and will, impose filtering rules and will monitor the use of school owned digital devices for inappropriate access to, or downloads from, websites. Breaches may lead to sanctions as described in the School Behaviour Policy and procedures and, in some cases, may involve the Police;

- understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school if there are problems or worries.

1.10 Parents

Parents play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local online safety campaigns/literature. The LGfL have produced a ready to use presentation for Parents which is free to download from https://lgfl.net/safeguarding/parent-online-safety .

The key responsibilities for parents are to:

- support the school in promoting online safety which includes the pupils' use of the Internet and the school's use of photographic and video images;
- work with and support the school when issues or concerns are identified which are as a result of the school's filtering and monitoring procedures and processes;
- read, sign, and promote the Pupil Acceptable Use Agreement and encourage their child to follow it;
- consult with the school if they have any concerns about their child'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) by ensuring that they themselves do not use the Internet/social network sites/other forms of technical communication in an inappropriate or defamatory way;
- support the school's approach to online safety by not uploading or posting to the Internet any images or details of others without permission and refraining from posting pictures, video or text that could upset, offend, or threaten the safety of any member of the school community or bring the school into disrepute.

12. Teaching and Learning

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk known as the 4Cs:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, including those generated using AI (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images) and online bullying; and,
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams. Any reports can be made to the Anti-Phishing Working Group.

Strong links between teaching online safety and the curriculum (see also Roles above) are the clearest in:

- Personal, Social and Health Education (PSHE)
- Relationships education, relationships, and sex education (RSE) and health
- Computing
- Citizenship

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 subject lead staff and making the most of unexpected learning opportunities as they arise. We will make reference to the DfE guidance 'Teaching online safety in schools' and the UKCIS guidance 'Education for a Connected World'.

Whenever overseeing the use of technology (devices, the Internet, new technology such as generative AI etc.) in school or setting as homework tasks, all staff will encourage sensible use, monitor (either physically; by the use of internet and web access software or via the use of active/proactive technology monitoring services) what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright, plagiarism, and data law.

We recognise that online safety and broader digital resilience must be included throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to assess the 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.

2.1 How internet use enhances learning

This school:

- has a clear, progressive online safety education programme as part of the Computing/PSHE curriculum. This covers the teaching of a range of skills and behaviours which are appropriate to the age and experience of the pupils concerned and include those to:
    - STOP and THINK before they CLICK;
    - develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - know how to narrow down or refine a search;
    - [for older pupils] understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - understand how photographs can be manipulated and how web content can attract unwanted or inappropriate attention;
    - 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;
    - understand why they must not post pictures or videos of others without their permission;
    - know not to download any files – such as music files – without permission;
    - have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] understand why and how some people will 'groom' children for sexual or extremist ideology reasons;
    - understand the impact of cyberbullying, making and sharing inappropriate images (including where generated by AI) and trolling and know how to seek help if they are affected by any form of online bullying;
    - know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through an end-user Acceptable Use Agreement which will be displayed throughout the school or when they log on to the school's network;
- ensures staff model safe and responsible behaviour in their own use of technology during lessons;

- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright/intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying online; online gaming/gambling etc.

2.2 Pupils with additional needs

We use a wide range of strategies to support children with additional needs who might need extra support to keep themselves safe, especially online.

- Sensitively check pupil's understanding and knowledge of general personal safety issues using reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.
- Apply rules consistently to embed understanding.
- Communicate rules clearly to parents and seek their support in implementing school rules at home. Working with parents and sharing information with them is relevant to all children, but this group especially.
- Careful explanations about why rules might change in different situations i.e. why it is ok to give your name and address to an adult if you are lost in town, but not when using the Internet.
- Consistent use of cause and effect linking the rules to consequences teaching realistic and practical examples of what might happen if… without frightening pupils.

2.3 Remote Education

The DfE expects schools to maintain their capabilities to deliver high quality remote education in cases where it is not possible or contrary to government guidance for some or all pupils to attend face-to-face education.

Our priority will always be to deliver high-quality face-to-face education to all pupils. Remote education will only ever be considered as a short-term measure and as a last resort where in person attendance is not possible.

This might include:

- occasions when our Head teacher decides that it is not possible for us to open safely, or that opening would contradict guidance from local or central government;
- occasions when individual pupils, for a limited duration, are unable to physically attend school but are able to continue learning, for example pupils with an infectious illness.

Information about how we organise and deliver remote education is available on request.

13. Handling online safety concerns and incidents

Our staff recognise that online safety is only one element of the wider safeguarding agenda as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

General concerns will be handled in the same way as any other child protection concern. Early reporting to the DSL is vital to ensure that the information contributes to the overall picture or highlights what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

Procedures for dealing with online safety, concerns and incidents are detailed in the following Policies:

- Child Protection Policy and procedures
- Behaviour Policy and procedures (includes anti-bullying procedures)
- Acceptable Use Agreements

- Prevent Risk Assessment
- Data Protection Policy, agreements, and other documentation (e.g. privacy statement, consent forms for data sharing image use etc.)

We are committed to taking all reasonable precautions to ensure online safety but recognise that incidents will occur both inside and outside school. All members of the school community are encouraged to report issues swiftly to school staff so that they can be dealt with quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL/DTL on the same day wherever possible or, if out of school, the following school day.

Any concern/allegation about misuse by staff or other adult in school will always be referred directly to the Head teacher unless the concern is about the Head teacher, in which case, the complaint will be directed to the Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline. Call 0800 028 0285 or email: help@nspcc.org.uk.

The school will actively seek support from other agencies as needed i.e., Cumberland Children Advice and Support Service (CASS), UK Safer Internet Centre's Professionals' Online Safety Helpline (0344 381 4772), NCA CEOP, Cumbria Police Prevent Officer, Cumbria Police, Internet Watch Foundation (IWF)). We will inform parents of online safety incidents involving their child and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or is considered illegal. See Sections below for procedures for dealing with the sharing of nudes and/or semi-nudes, upskirting and online (cyber) bullying.

- In this school there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions.
- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The DSL will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy and procedures for dealing with concerns.
- The DSL will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The school will manage Online Safety incidents in accordance with the school discipline/Behaviour Policy where appropriate.
- The school will inform parents of any incidents or concerns as and when required unless doing so would put a child at increased risk of harm.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place or the school is unsure how to proceed with an incident then the school will contact the CASS **and** escalate the concern to the Police.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

Incidents will be dealt with as soon as possible in a proportionate manner through normal behaviour/disciplinary procedures. It is important that, where necessary, members of the school community are made aware that incidents have been dealt with.

3.1 Sharing nudes and/or semi-nudes

Where incidents of the making or sharing of nudes and/or semi-nudes (including where generated by AI) via the internet or mobile phone by those under the age of 18 are discovered , we will refer to the UK Council for (UKCIS) guidance 'Sharing nude and semi-nude images'. A copy of this document is available

from the school office. Where one of the parties is over the age of 18 and the other is under 18, we will refer to it as child sexual abuse and report in accordance with our Child Protection Policy and procedures.

All staff and other relevant adults have been issued with a copy of the UKCIS overview document (Sharing nudes and semi-nudes: how to respond to an incident) in recognition of the fact that it is generally someone other than the DSL who will first become aware of an incident. Staff, other than the DSL, must not intentionally view, copy, print, share, store or save or delete the image or ask anyone else to do so but must report the incident to the DSL as soon as possible.

It is the responsibility of the DSL to follow the guidance issued by UKCIS, decide on the next steps and whether to involve other agencies as appropriate.

It is important to understand that whilst the sharing of nudes and/or semi-nudes is illegal, pupils should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue.

The UKCIS advice outlines how to respond to an incident of nudes and semi-nudes being shared including:

- risk assessing situations;
- safeguarding and supporting children;
- handling devices and images;
- recording incidents, including the role of other agencies.
- informing parents

The types of incidents which this advice covers are:

- a person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18;
- a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18;
- a person under the age of 18 is in possession of nudes and semi-nudes created by another person under the age of 18.

3.2 Upskirting

All staff are aware that 'upskirting' (taking a photo of someone under their clothing) is now a criminal offence, but that pupils should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue. If staff or other adults become aware of an incident of 'upskirting', the issue must be reported to the DSL as soon as possible.

3.3 Cyberbullying

Cyberbullying (also known as online bullying) can be defined as the use of information and communications technology particularly mobile devices and the internet, deliberately to upset someone else and reported incidents will be treated in the same way as any other form of bullying. The Behaviour Policy and procedures will be followed in relation to sanctions taken against the perpetrator. It is important not to treat online bullying separately to offline bullying and to recognise that some bullying will have both online and offline elements. Support will be provided to both the victim and the perpetrator. In some cases, it may be necessary to inform or involve the Police.

Many children and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming, or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that children, school staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are several statutory obligations on schools in relation to behaviour which establish clear responsibilities to respond to bullying. In particular, section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's Behaviour Policy which must be communicated to all pupils, school staff and parents;
- gives Head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on in line with the school Behaviour Policy and procedures.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed, they should seek assistance from the Police.

All staff have a role in implementing our behaviour policy and our procedures for tackling cyberbullying as follows, and are encouraged to use Resources | Childnet which offers guidance and practical advice (select the topic online bullying):

- Cyberbullying (along with all other forms of bullying) of any member of the school community will never be tolerated. Full details are set out in the Behaviour Policy and procedures.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff, and parents will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the perpetrator, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the Police, if necessary.
- Pupils, staff, and parents will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos.
- Sanctions for those involved in cyberbullying may include:
  - The perpetrator will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content if the perpetrator refuses or is unable to delete content.
  - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the Behaviour Policy and procedures, Acceptable Use Agreement and Disciplinary Procedures.
  - Parents of both the perpetrator(s) and the victim(s) will be informed.
  - The Police will be contacted if a criminal offence is suspected.

3.4 Harmful online challenges or hoaxes

An online challenge will generally involve users recording themselves taking a challenge and then distributing the resulting video through social media sites, often inspiring or daring others to repeat the challenge. Whilst many will be safe and fun, others can be potentially harmful and even life threatening.

If staff are confident children are aware of, and engaged in, a real challenge that may be putting them at risk of harm, then it would be appropriate for this to be directly addressed by either the DSL or a senior leader in school. Careful consideration will be given on how best to do this, and it may be appropriate to offer focussed support to a particular age group or individual children at risk. We will take account of the fact that even with real challenges, many children may not have seen it and may not be aware of it and will carefully weigh up the benefits of institution-wide highlighting of the potential harms related to a challenge against needlessly increasing children's exposure to it.

Where staff become aware of a potentially harmful online hoax or challenge, they will immediately inform the DSL who will take the appropriate action either with the pupil concerned or with the wider group where the incident involves more than one pupil.

Where the DSL considers it necessary to directly address an issue, this can be achieved without exposing children to scary or distressing content. In the response, we will consider the following questions:

- is it factual?
- is it proportional to the actual (or perceived) risk?
- is it helpful?
- is it age and stage of development appropriate?
- is it supportive?

A hoax is a deliberate lie designed to seem truthful. The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children to be spread quickly.

We will carefully consider if a challenge or scare story is a hoax. Generally speaking, naming an online hoax, and providing direct warnings is not helpful. Concerns are often fuelled by unhelpful publicity, usually generated on social media, and may not be based on confirmed or factual occurrences or any real risk to children. There have been examples of hoaxes where much of the content was created by those responding to the story being reported, needlessly increasing children's exposure to distressing content.

Evidence from Childline shows that, following viral online hoaxes, children often seek support after witnessing harmful and distressing content that has been highlighted, or directly shown to them (often with the best of intentions), by parents, schools, and other bodies. In this respect, staff will be mindful of the advice provided by the UK Safer Internet Centre which provides guidance on dealing with online hoaxes or challenges.

In any response, reference will be made to the DfE guidance 'Harmful online challenges and online hoaxes'.

3.5 Harmful sexual behaviour, sexual violence and harassment

DfE guidance on harmful sexual behaviour (HSB), sexual violence and harassment is referenced in Part five of 'KCSiE'. All staff are aware of this guidance.

We have a zero tolerance approach to all forms of HSB, sexual violence and harassment and will act appropriately on information which suggests inappropriate behaviour regardless of the considered seriousness. Any incident of HSB, sexual harassment or violence (online or offline) must be reported to the DSL at the earliest opportunity. The DSL will follow the guidance as outlined in the Child Protection Policy and procedures. Sanctions will be applied in line with our Behaviour Policy and procedures.

3.6 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 rules are defined in the relevant Acceptable Use Agreements as provided to pupils, staff, and Governors.

Where pupils contravene these rules, the Behaviour Policy and procedures will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct and, where necessary, the school disciplinary procedures.

The school reserves the right to withdraw, temporarily or permanently, any or all access to such technology or the right to bring mobile technology devices onto school property.

3.7 Social media incidents

See also Section 9. below. Social media incidents are governed by Acceptable Use Agreements. Breaches will be dealt with in line with these procedures, the Behaviour Policy and procedures (for pupils) and the staff Code of Conduct/Disciplinary procedures (for staff and other adults).

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by an identifiable member of the school community, we will request that the post be deleted and will expect this to the actioned promptly.

Where an offending post has been made by a third party or is anonymous, the school may report it to the hosting platform, the Police or may contact the Professionals' Online Safety Helpline (UK Safer Internet Centre) for support or assistance in accelerating the process of removal.

14. Data protection and data security

All pupils, staff, Governors, parents, and other adults working in or visiting school are bound by the school's Data Protection Policy and procedures a copy of which is available from the school office.

There are references to the relationship between data protection and safeguarding in key DfE documents i.e. KCSiE and Data protection: a toolkit for schools which the DPO and DSL will seek to apply.

The Head teacher, DPO and Governors work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always the primary consideration and data protection processes support careful and legal sharing of information. The Data Protection Act 2018 does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with the DPA. Legal 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. 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. As with all data sharing, appropriate organisational and technical safeguards will be in place.

All pupils, staff, Governors, volunteers, contractors, and parents are bound by the school's Data Protection Policy and procedures.

4.1 Maintaining Information Systems Security

Local Area Network (LAN) security issues include:

- Users must act reasonably e.g. the downloading of large files or viewing sporting events during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For staff, flouting the school Acceptable Use Agreement may be regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers will be located securely and physical access restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network is installed and current.
- Access by wireless devices will be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Broadband firewalls and local CPEs (Customer Premises Equipment) are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made in partnership between school and our network provider.

The following statements apply in our school:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.

- Use of user logins and passwords to access the school network will be enforced – see Section 6.2 below.

The school broadband and online suppliers are System IT.

The Head teacher, Data Protection Officer and Governors work together to ensure a DPA 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.

4.2 Password Security

We will ensure that the school network is as safe and secure as is reasonably possible and that users can only access data to which they have right of access; no user is able to access another's files without permission (or as allowed for monitoring purposes within the school's procedures); access to personal data is securely controlled in line with the school's personal data procedures; logs are maintained of access by users and of their actions while users of the system.

All users (adults and children) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated . Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

Users will change their passwords every 90 days.

Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This will apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password security procedures:

- at induction;
- through the school's Online Safety Policy and procedures;
- through the Acceptable Use Agreement.

Pupils will be made aware of the school's password security procedures:

- in Computing/ICT and/or Online Safety lessons;
- through the Acceptable Use Agreement.

The following rules apply to the use of passwords:

- passwords must be changed every 90 days;
- the last four passwords cannot be re-used;
- the password will be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
- the account should be "locked out" following six successive incorrect log-on attempts;
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption);
- requests for password changes should be authenticated by Alison Cattanach to ensure that the new password can only be passed to the genuine user.

The "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) are made available to the Head teacher or other nominated senior leader and kept in a secure place.

Audit/Monitoring/Reporting/Review:

The responsible person Alison Cattanach will ensure that full records are kept of:

- User Ids and requests for password changes;
- User log-ons;
- Security incidents related to this Policy and procedures.

In the event of a serious security incident, the Police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by Digital technology lead at regular intervals.

15. Electronic Communications

5.1 Managing Email

Our general principles for email use are as follows:

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive an offensive email or one which upsets or worries them.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Staff will only use official school provided email accounts to communicate with pupils and parents, as approved by the SLT. Any deviation from this must be agreed with the Head teacher.
- Any digital communication between staff and pupils or parents (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications. 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 Head teacher (if by a staff member).
- Staff are not permitted to use personal email accounts during school hours or for professional purposes.
- Pupils and staff are/are not [delete as appropriate] permitted to use the school email system for personal use and 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.
- 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.
- Users must immediately report to the Head teacher or DSL the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and **must not** respond to any such email.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information must not be posted on the school website and only official email addresses will be used to identify members of staff.
- Spam, phishing, and virus attachments can make email dangerous. The school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

5.2 Emailing personal, sensitive, confidential, or classified information

Staff or pupil personal data should never be sent/shared/stored in emails and any data must be encrypted prior to being sent.

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible;
- The use of Hotmail, BTInternet, G-mail or any other Internet based webmail service for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by email;
  - Exercise caution when sending the email and always follow these checks before releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information;
    - Verify (by phoning) the details of a requestor before responding to email requests for information;
    - Do not copy or forward the email to any more recipients than is necessary.
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
  - Send the information as an encrypted document **attached** to an email;
  - Provide the encryption key or password by a **separate** contact with the recipient(s) e.g. by telephone or in writing;
  - Do not identify such information in the subject line of any email;
  - Request confirmation of safe receipt.

5.3 Zombie accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left;
- Prompt action on disabling accounts will prevent unauthorised access;
- Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days).

Staff will refer to further advice available at IT Governance as necessary.

16. 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. Rachel Blair has day to day editorial responsibility for online content published by the school on the school website and will ensure that content published is accurate and appropriate. The school website is managed by/hosted by Primary site.

The DfE has determined information which must be available on a school website - What maintained schools must or should publish online.

Where other staff submit information for the website, they are asked to consider the following principles:

- The contact details on the website are the school address, email, and telephone number. Staff, Governors, or pupils' personal information are not published.
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT').
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy procedures and copyright.
- Where pupil work, images or videos are published on the website, their identities are protected, and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

17. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, pupils and parents need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

- We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent. Parents are required to inform the school if their consent changes.
- We seek consent for the publication of images from pupils.
- When we publish images or video, we will inform pupils and parents before publishing, so they have a chance to object as is their legal right under DPA 2018.
- We do not identify pupils in online photographic materials or include the names (full or partial) of pupils in the credits of any published school produced digital materials. Photo file names/tags do not include full names to avoid accidentally sharing them. All metadata (e.g. EXIF data) is removed from the images to reduce the risk of revealing location, device details or timestamps.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. 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.
- Staff are governed by their contract of employment, the staff Code of Conduct and sign the school's Acceptable Use Agreement. This includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Staff are permitted to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution, and publication of those images. Those images will, wherever possible only be taken on school equipment. Members of staff may occasionally use personal phones to capture photos or videos of pupils. These will be appropriate, linked to school activities, taken without secrecy, and not captured in a one-to-one situation. Photos will always be moved to school storage as soon as possible after which they are deleted from personal devices and/or cloud services (Note: many phones automatically back up photos).
- Staff will ensure that when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. It is considered good practice to only share photos taken from a distance, blurred images or images taken from over the shoulder.
- Digital images/videos are stored on the school network in line with the retention schedule of the school Data Protection Policy.
- Pupils are taught about how images can be manipulated in their online safety education programme and are taught to consider how to publish for a wide range of audiences which might include Governors, parents, or younger children as part of their ICT scheme of work;
- Pupils are taught that they should not post images or videos of others without their consent. 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, such as house number, street name or school. 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.
- Staff and parents are regularly reminded about the importance of not sharing without consent, due to child protection concerns (e.g. children looked-after often have restrictions for their own protection) data protection, religious or cultural reasons or simply for reasons of personal privacy.

- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil consent for its long-term use (for more information see KAHSC Safety Series: General G21 – The Use of Images when Working with Children and the KAHSC Model Consent Form - trips images and pain relief).
- A pupil's work can only be published with the consent of the pupil and parents. We will seek the consent of the pupil first and then, if necessary, the parents.

18. Cloud Platforms

This school adheres to the principles of the DfE documents Cloud computing services: guidance for school leaders, school staff and governing bodies, Meeting digital and technology standards in schools (Cloud solution standards for schools and colleges. Our Data Protection Policy and procedures includes the use of Cloud services.

For online safety, basic rules of good password management, expert administration and training is used to keep staff and pupils safe and to avoid incidents. The DPO and network manager will analyse and document systems and procedures before they are implemented and regularly review them.

The following principles apply:

- Privacy statements inform parents and children when and what type 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 on the basis of a data protection impact assessment (DPIA).
- 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 consent.
- Only school-approved platforms are used by students or staff to store pupil work.
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

19. Social Media

9.1 Managing social networking, social media, and personal publishing sites

This school operates on the principle that if we don't manage our social media reputation, someone else will. Online reputation management is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Negative coverage almost always causes some level of disruption and can result in distress to individuals.

We therefore manage our social media footprint carefully to know what is being said about the school and in order to respond to criticism and praise in a fair, responsible manner.

The school has an official Facebook account which is managed by the school and will respond to general enquiries about the school, but we ask parents not to use these channels to communicate about their children or other personal matters.

Email (via governor, staff, and pupil school email addresses only) is the official online communication channels between parents and the school, and between staff and pupils. While we welcome communication about and with us from within and outside our school community online using our social media accounts, they **must never** be used to communicate with us about personal or private matters, including over any private messaging service operated by such social media providers.

Staff, pupils', and parents' Social Media presence:

Social media 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 Agreements and our Behaviour Policy and procedures 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 derogatory or inappropriate or which might bring the school, student body or teaching profession into disrepute. This applies to both 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 us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure (available via the school website) 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.

Many social media platforms have a minimum age of 13 but the school regularly deals 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 accept that there is a balance between not encouraging underage use whilst at the same time 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, abuse or exploitation. However, children will often learn most from the models of behaviour they see and experience. Parents can best support this by talking to their children about the apps, sites, and games they use, with whom, for how long, and when (late at night is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Pupils are not allowed[1] to be 'friends' with or make a 'friend request' to any staff, Governors, volunteers or regular school contractors or otherwise communicate via social media. Pupils are discouraged from 'following' staff, Governors, volunteers, or regular school contractors public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be difficult to control. This, however, highlights the need for staff to remain professional in their private lives. Conversely staff must not follow public pupil accounts.

Staff are reminded that they should not bring the school or profession into disrepute and the best way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. Staff must never discuss the school or its stakeholders on social media and ensure that their personal opinions are not attributed to the school.

The following principles apply:

- This school will take steps to control access to social media and social networking sites over school networks, on school-owned devices, and on social media or other online accounts we control.
- Appropriate guidance or signposting will be provided for pupils, parents, Governors, staff, and volunteers about Social Media and how to use it safely - NCSC.GOV.UK, Social Media - UK Safer Internet Centre, and Social media, online communities and safeguarding | NSPCC Learning.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests, and clubs etc.
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the SLT before using Social Media tools in the classroom.
- Staff official blogs or wikis will be password protected and run from the school website with approval from the SLT. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

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

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, or defamatory.
- Steps will be taken in line with guidance on How schools and parents can spot and tackle online abuse of teachers - The Education Hub (blog.gov.uk).
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding a pupil's use of social networking, social media, and personal publishing sites (in or out of school) will be raised with their parents, particularly when concerning the underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and outlined in the school Staff Acceptable Use Agreement – see link on contents page.

9.2 Personal devices and bring your own device (BYOD) procedures

We recognise the widespread use of personal devices makes it essential that schools take steps to ensure mobile phones and devices, including wearable or "smart" technologies like health or fitness trackers, meta glasses etc. (some of which are capable of taking and storing digital images), are used responsibly at school and it is essential that pupil use of their devices does not impede teaching, learning and good order in classrooms. Staff will be given clear boundaries on professional use and these are set out in the staff Code of Conduct.

Mobile/wearable devices can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to sexual harassment, cyberbullying, and other forms of control;
- Apps or mobile devices which broadcast location data can make staff or pupils vulnerable to behaviours like stalking and can provide perpetrators with information to take cyberbullying into the real world.
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering;
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, cyberbullying, and data protection issues in relation to inappropriate capture, use or distribution of inappropriate images of pupils or staff;

Permitted use of mobile phones and personal devices is a school decision and the following will apply:

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the relevant school Acceptable Use Agreement, staff Code of conduct.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school Behaviour Policy and procedures.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable materials, including those which promote pornography, violence, or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.
- School staff may confiscate a phone or device if they believe it is being used to contravene the Behaviour Policy and procedures.
- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the Police for further investigation.
- Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent whilst in the school.

- The recording, taking, and sharing of images, video and audio on any mobile phone or other personal device is not permitted, except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is authorised to withdraw or restrict authorisation for use at any time if it is deemed necessary. Where permission is given by the Head teacher, no images or videos are to be taken on mobile phones or personally owned mobile devices without the prior consent of the person or people in the image.
- The Bluetooth function of a mobile phone should always be switched off and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft, or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break time.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets, and swimming pools.

Pupil use of personal devices:

- The school procedure for the use of mobile phones states that pupil mobile phones should not be brought into school. However, the school accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. If this is the case, the circumstances should be discussed with the class teacher and the normal rules regarding use during the school day will apply.
- If a pupil breaches the school procedures, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents in accordance with the school Behaviour Policy and procedures.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parent, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Pupils will be provided with school mobile phones or other hand-held personal devices to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices:

- Staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents is required.
- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off, location data switched off unless being used only for the duration of a specific task like route directions on a school trip, and mobile phones or personally owned devices will not be used during teaching periods unless permission has been given by a member of SLT for emergency circumstances.
- The function on a personal device which allows the capture and recording of images including photographs, video, and voice will be disabled whilst on the school site.

- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the SLT.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Where members of staff are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide their own mobile number for confidentiality purposes.
- If a member of staff breaches the school Policy and procedures, then disciplinary action may be taken.

Parents are asked to keep phones out of sight whilst on the school premises. They must 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 are not allowed networked file access via personal devices. However, they are permitted to access the school wireless internet network for school-related internet use/limited personal use within the framework of the Acceptable Use Agreement. All such use is monitored.

Searching, Screening and Confiscation

In line with the DfE guidance '[Searching, screening and confiscation: guidance for schools]', the Head teacher and staff authorised by them have a statutory power to search pupils/property on school premises (with consent for items banned by the school and without consent for items which are prohibited or illegal). Staff may examine any data or files on an electronic device they have confiscated as a result of a search, if there is good reason to do so. If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff must never intentionally view the image, and must never copy, print, share, store, save or delete such images.

When an incident might involve an indecent image and/or video of a child, the member of staff will confiscate the device, avoid looking at the device and refer the incident to the DSL (or deputy) as the most appropriate person to advise on the school's response. 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, upskirting, violence or bullying. Further details are available in the Behaviour Policy and procedures.

110. Generative Artificial Intelligence

Generative artificial intelligence (AI) is technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. ChatGPT and Google Bard are generative AI tools built on large language models (LLMs).

Tools such as ChatGPT and Google Bard can:

- answer questions;
- respond to prompts in a human-like way
- complete written tasks

Other forms of generative AI can produce:

- audio
- images
- simulations
- code
- text
- videos

AI technology is not new and we already use it in everyday life for:

- email spam filtering
- media recommendation systems
- navigation apps
- online chatbots

However, recent advances in technology mean that we can now use tools such as ChatGPT and Google Bard to produce AI-generated content. This creates both opportunities and challenges for schools which are briefly described in DfE guidance 'Generative artificial intelligence (AI) in education' and 'Using AI in education settings: support materials'. DfE guidance 'Generative AI: product safety expectations' outlines the capabilities and features that generative artificial intelligence (AI) products and systems should meet to be considered safe for users in our setting.

All staff who make any use of AI are expected to have read the DfE guidance (see links above) and must incorporate the principles in all of their work with it. All work with AI must also be done in line with this Policy and our Data Protection Policy. New uses of AI that are not similar to anything we currently do must be explained to and approved by the Head Teacher who will lead on deciding whether the benefits outweigh the risks and how the risks will be monitored and minimised.

111. Managing filtering and monitoring

For specific information on how we manage filtering and monitoring in this school, please see **Appendix A**.

Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn we (the Governors, SLT and staff) will do all we reasonably can to limit children's exposure to online safety risks from the school's IT system. As part of this process, we will ensure that the school has appropriate filtering and monitoring systems in place and ensure that a review of their effectiveness is carried out at least once every academic year. Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's DSL and IT support. The annual review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. A record will be kept of these checks.

By making use of an appropriate risk assessment, the school will work towards meeting the obligations set out in the DfE filtering and monitoring standards.

The Governors will review the standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting the standards.

Filtering on school networks must not be tested by searching for content that is known to be filtered because it is harmful. South West Grid for Learning (swgfl.org.uk) have created a tool to check whether a school's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content Your Internet Connection Blocks Child Abuse & Terrorist Content).

112. Webcams and Surveillance Camera Systems (incl. CCTV)

The school uses a surveillance camera system for security and safety. The only people with access to the surveillance camera system are staff. Notification of camera system use is displayed at the front of the school and at various points throughout the building so that individuals are aware that a surveillance camera system is in operation. Staff will refer to the Information Commissioner (IC) web pages for further guidance and the school surveillance camera system procedures.

In relation to webcams:

- We do not use public (unrestricted) access webcams in school unless we are livestreaming an appropriate educational project such as construction work or egg-hatching in a way that does not capture images of children or adults and positioning is checked regularly e.g., disabling any microphone, and siting the camera so only the eggs are visible, or so far away from construction work that people are not identifiable.
- We only use private (restricted) access webcams with children or adults when it is necessary e.g., for

educational purposes or school management reasons (commonly remote education, Teams meetings between colleagues and other professionals, and live online training platforms) and when we have conducted a DPIA which indicates it is reasonable to and that recordings or streaming will be appropriately secure.

- All webcams that are not in use are covered and access to the device's microphones is disabled so that if accessed in an unauthorised way, it will not function to broadcast anything.
- Misuse of the webcam by any member of the school community will result in sanctions.
- Webcams can be found on staff computers Notification is given in this/these area(s) filmed by webcams by signage.
- As for all images, content captured by webcams can only be published if pupil and parental consent is valid.

113. Managing emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration, and multimedia tools. We will undertake a risk assessment on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safe practice has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Instagram, YouTube, X and Tik Tok. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication but is often not possible. Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

We will take steps to keep updated on new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For example, whether communicating with a pupil or families via SMS or an instant messaging app about a pupil's absence or to send reminders is appropriate in some or all cases. There are dangers for staff if personal devices or accounts are used to contact pupils so, we will endeavour to make a school owned device or account available if this kind of contact is necessary.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school Policy and procedures. Abusive messages should be dealt with in line with the school's Behaviour Policy and procedures.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

114. Cyber security and resilience

It is vital that we understand our vulnerabilities in relation to potential cyber-attacks and breaches, regularly review our existing defences and take the necessary steps to protect our networks. As well as having a current and cohesive Cyber Response Plan in place, there are several measures that we can implement to help to improve our IT security and mitigate the risk of a cyber-attack. These measures fall

under the 'Identify, Protect and Detect' pillars of effective cyber resilience and are outlined in our cyber security and resilience strategy. We make use of the DfE 'Cyber security standards for schools' to assist us to improve our resilience against cyber-attacks. A copy of our cyber security strategy is available on request from the school office.

115. Policy Decisions

15.1 Authorising internet access

The school will allocate internet access to staff and pupils based on educational need. It will be clear who has internet access and who has not. Normally most pupils will be granted internet access. We will not prevent pupils from accessing the Internet unless the parents have specifically denied permission, or the child is subject to a sanction as part of our Behaviour policy and procedures.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the Staff Acceptable Use Agreement before using any school ICT resources.
- Parents will be asked to read and sign the School Acceptable Use Agreement for pupil access and discuss it with their child, where appropriate.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to Setting Type:

- At EYFS and Key Stage 1, pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2, pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

15.2 Assessing risks

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

Risks can be considerably greater where tools are used which are beyond the school's control such as most popular social media sites.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from internet use.
- The school will audit ICT use to establish if the Online Safety Policy and procedures is adequate and that the implementation of the Online Safety Policy is appropriate – see LGfL Online Safety Audit.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police using 101 or the appropriate online report from available from our local Constabulary website.
- Methods to identify, assess and minimise risks will be reviewed regularly.

15.3 Responding to incidents of concern

Refer to Section 3 above.

116. Communicating Policy and procedures

16.1 Introducing the Policy and procedures to Pupils

Many pupils are very familiar with the culture of mobile and internet use, so we try to involve them in the development of the School Online Safety Policy, through "pupil voice" activities like the School Council. As pupils' perceptions of the risks will vary, the online safety rules will be explained or discussed in an age-appropriate manner.

Online safety pupil and parental engagement programmes we can use include:

- Think U Know (now part of CEOP)
- Childnet

Pupil induction and ongoing training and education will include:

- Informing all users that network and internet use will be monitored.
- Establishing an online safety training programme across the school to raise the awareness and highlight the importance of safe and responsible internet use.
- Pupil instruction regarding responsible and safe use *before* internet access is given.
- An online safety module in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Online safety training as part of the transition programme across the Key Stages and when moving between schools or other educational or training settings.
- Accessible Online Safety rules or copies of the pupil Acceptable Use Agreement including posters in all rooms with computers/internet access.
- Regular reinforcement of safe and responsible use of the Internet and technology across the curriculum, in all subject areas, and extended schools or extra-curricular activities.
- Particular attention paid to Online Safety education where pupils are considered to be vulnerable.

16.2 Discussing the Policy and procedures with Staff

It is important that all staff feel confident meeting the demands of using ICT appropriately in teaching, administration, and all other aspects of their school and personal life and the School Online Safety Policy and procedures will only be effective if all staff subscribe to its values and methods.

Staff will be given opportunities to discuss the issues and develop appropriate teaching or other work strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an internet activity without preparation.

Any member of staff who has concerns about any aspect of their own or anyone else's ICT or internet use either on or off site, they should discuss this with their line manager. Where concerns are related to children's safeguarding, they should also be reported to the DSL who should follow the Child Protection Policy and procedure for recording and reporting allegations that meet the harm threshold and recording (and in some case reporting i.e. to a contractor's employer) low level concerns that do not.

Consideration is given when members of staff are provided with devices by the school which may be accessed outside of the school network. Staff are made aware of their responsibility to maintain the security and confidentiality of school information.

All staff have a universal duty to understand harms and protect children from them, including online. ICT use is widespread and all staff including administration, midday supervisors, facilities staff, Governors, and volunteers who use it or work with children who use it are included in awareness raising and training.

Induction of all new staff will include:

- A copy of the Online Safety Policy and procedures and a scheduled opportunity to discuss them.
- That internet traffic can be monitored and traced to the individual user, and the importance of having high professional standards and always following current policies and procedures.

- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally.
- Requirement to read, understand and sign relevant Acceptable Use Agreements.
- For staff who manage filtering systems or monitor ICT use: that they will be supervised by the SLT and what the procedures for reporting issues are.
- How the school will promote online tools which staff should use for work purposes, especially with children, and the procedure staff should go through if there is a new tool they want to use.
- That their online conduct out of school could have an impact on their role and reputation in school. Civil, legal, or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Volunteers will receive an online safety induction based on what staff receive but suitable for the role they have been asked to fulfil.

When we employ an Early Career Teacher (ECT replacing newly qualified teacher or NQT) or work with trainee teachers the DTL will ensure use of the UKCIS Online Safety Audit Tool or similar self-assessment with them to help them better understand their role in keeping children safe online and our policy and practice.

LGfL produce a vast number of resources including information on Generative AI available from https://lgfl.net/safeguarding/resources

16.3 Enlisting Parents' Support

Internet use in pupils' homes is increasingly widespread. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks.

To engage with parents we will:

- draw attention to our Online Safety Policy and procedures in newsletters, and on the school website;
- Advise parents on the details of the behaviour policy and educate pupils about the risks associated with the use of mobile phones both in school and more broadly, and the benefits of a mobile phone-free school environment;
- encourage a partnership approach to online safety at home and at school which may include demonstration evenings, regular suggestions for safe home internet use, promoting educational online safety activities for families, or highlighting online safety issues at other attended events e.g. parent evenings and sports days;
- ask parents to read and sign the school Acceptable Use Agreement for younger pupils and discuss its implications with their children and offer support to do this if required;
- provide information and guidance for families about on online safety in a variety of formats;
- provide advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet;
- refer interested parents to organisations listed in the "Online safety Links";
- advise that they check whether their child's use of the Internet elsewhere in the community is covered by an appropriate Acceptable Use Agreement and if they understand the rules.

117. Complaints

The school will take all reasonable precautions to ensure 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 materials will never appear on a school computer or mobile device. Neither the school staff nor the Governing Body can accept liability for material accessed, or any consequences of internet access.

- Complaints about the misuse of on-line systems will be dealt with under the school's Complaints procedure.

- Complaints about cyberbullying are dealt with in accordance with our Anti-bullying procedures which form part of our Behaviour Policy and procedures.
- Complaints related to child protection are dealt with in accordance with school Child Protection Policy and procedures.
- Any complaints about staff misuse will be referred to the Head teacher.
- All online safety complaints and incidents will be recorded by the school including any actions taken making use of the 'Response to online safety incidents or concerns' flowchart.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by class teacher/Head teacher;
- informing parents;
- removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework);
- referral to the Police.

Appendix A

Richmond Hill School - Online Safety - Filtering and Monitoring Arrangements

1. Introduction

The Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education' (KCSiE) obliges schools in England to "ensure appropriate filters and appropriate monitoring systems are in place and ensure that a review of their effectiveness is carried out at least once every academic year. Reviews should be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's DSL and IT support. They should include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record should be kept of these checks." In addition, schools "should be doing all that they reasonably can to limit children's exposure to risks from the school's IT system" however, we will "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."

To further support schools to meet digital and technology standards, the DfE have published Filtering and Monitoring Standards. (See 2. Below). In addition to aspects of both filtering and monitoring systems, these standards detail the allocation of roles and responsibilities, and that schools should be checking their filtering and monitoring provision at least annually including . Given the extent of personal data involved with some monitoring solutions, we will consider undertaking a data protection impact assessment and ensure that the adopted monitoring strategy is integrated within our policies and alongside relevant data sharing agreements.

'KCSiE' also requires that **all** staff should receive, at induction, appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring). The training will be regularly updated. In addition, all staff receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety, including arrangements for filtering and monitoring, empowers the school to protect and educate pupils, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, including those generated using AI (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images) and online bullying; and,

Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams. Any reports can be made to the Anti-Phishing Working Group.

Filtering and monitoring systems are used to keep pupils safe when using the school's IT system. Filtering systems block access to harmful sites and content. Monitoring systems identify when a user accesses or searches for certain types of harmful content on school devices (it doesn't stop someone accessing it). The school is then alerted to any concerning content so that appropriate interventions and ultimate responses can be made.

All staff and others who can access school devices will be provided with a copy of the school Code of Conduct on induction which sets out information in relation to the acceptable behaviour standards, including those for use of school devices (either in school or off-site). All staff, pupils (or parents on the child's behalf) and Governors will be required to read and sign the Online Acceptable Use agreement on induction for the use of school devices (either in school or off-site).

12. DfE Filtering and monitoring standards

The school will comply with the requirements set out in DfE guidance relating to 'Filtering and monitoring standards for schools and colleges', which are summarised in figure 1 below:

Required Outcome	**Responsibility**	**Named responsible individual(s)**
Identify and assign a member of the Senior Leadership Team (SLT) to be responsible for ensuring that the standards are met.	Governors	Rachel Blair
Identify and assign a Governor to be responsible for ensuring that the standards are met.	Governors	Amanda Coates
Identify and assign the roles and responsibilities of staff (e.g. school Digital Technology Lead/Designated Safeguarding Lead) and third parties (e.g. external service providers).	Governors	Amanda Coates
Document decisions about what is blocked or allowed and why.	SLT	Rachel Blair, Megan Oneil, Laura Vailionis, Conor Merone
Review the effectiveness of our provision (and provide evidence e.g. communication between technical staff and Designated Safeguarding Leads (DSLs).	SLT	Rachel Blair, Megan Oneil, Laura Vailionis, Conor Merone
Oversee reports.	SLT	Rachel Blair Megan Oneil, Laura Vailionis, Conor Merone
Ensuring all staff have received appropriate and up to date training, follow Policies, procedures and processes around online safety and filtering and monitoring.	SLT	Rachel Blair Megan Oneil, Laura Vailionis, Conor Merone
Ensuring all staff act on reports and concerns.	SLT	Megan Oneil, Laura Vailionis, Conor Merone
Oversee and act on filtering and monitoring reports.	DSL	Rachel Blair
Oversee and act on safeguarding concerns.	DSL	Rachel Blair
Oversee and act on checks to monitoring systems.	DSL	Rachel Blair
Maintain filtering and monitoring systems.	IT service provider	System IT
Provide filtering and monitoring reports.	IT service provider	System IT
Complete actions following concerns or checks to systems.	IT service provider	System IT
Carry out reviews of the filtering and monitoring provision at least annually.	JOINT (Govs, SLT, DSL, and IT provider)	

Carry out checks which are informed by the review to ensure systems are working as intended.	JOINT (Govs, SLT, DSL, and IT provider)

Figure 1: Filtering and monitoring standards – summary of requirements.

In order to meet these requirements we will ensure that the following arrangements are in place at the outset.

We will identify and assign roles and responsibilities to manage our filtering and monitoring systems as follows and outlined above:

- A member of SLT and a Governor will be responsible for ensuring the standards are met.
- The roles and responsibilities of individual staff members (e.g. pastoral leads, DTL, DSL) and third parties (e.g. external service providers such as IT providers) will be clearly identified.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers. All decisions regarding what content is blocked or allowed, and why, will be documented.
- All staff will be given awareness training at induction outlining how our filtering and monitoring systems work. This training will also be included in the annual safeguarding training.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The Head teacher/DSL works closely together with IT service providers to meet the needs of our setting.

The Head teacher/DSL takes lead responsibility for safeguarding and online safety, in the following areas:

- filtering and monitoring reports;
- safeguarding concerns;
- checks to filtering and monitoring systems.

The Head teacher/IT service provider has technical responsibility for:

- maintaining filtering and monitoring systems;
- providing filtering and monitoring reports;
- completing actions following concerns or checks to systems.

The Head teacher and IT service provider work to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

13. Blocking harmful and inappropriate content

No filtering system can be 100% effective and we understand the coverage of our filtering system, any limitations it has, and take mitigating measures accordingly to minimise harm and to meet our statutory duties outlined in KCSiE and the Home Office Prevent Duty.

We will ensure that our filtering system blocks harmful and inappropriate content, including all sites on the Internet Watch Foundation (IWF) list, without unreasonably impacting teaching and learning or restricting students from learning how to assess and manage risk themselves. As a minimum we will ensure that our filtering system manages the following content (and web search)

Content	**Explanatory notes – content that:**
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances.

Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.
Gambling	Enables gambling.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.
Pornography	Displays sexual acts or explicit images.
Piracy and copyright theft	Includes illegal provision of copyrighted material.
Self-Harm	Promotes or displays deliberate self-harm (including suicide and eating disorders).
Violence	Displays or promotes the use of physical force intended to hurt or kill.

Figure 2: Filtering systems - inappropriate online content (reproduced from UKSIC guidance)

In order to ensure that our filtering system blocks harmful and inappropriate content the following arrangements will apply:

- the Governing Body will support SLT to procure and set up systems which meet this standard and the risk profile of the school;
- we will follow the guidance set out for schools by the UK Safer Internet Centre (UKSIC) on 'Appropriate Filtering for Education Settings' to inform our approach to establishing appropriate levels of filtering;
- we will ensure that our filtering provider is a member of the Internet Watch Foundation; is signed up to the Counter-Terrorism Internet Referral Unit list (CTIRU) and blocks access to illegal content including child sexual abuse material (CSAM);
- we will ensure that our filtering system is operational, up to date and applied to all users (including guest user accounts); school owned devices and devices using the school broadband connection;
- our filtering provider will be asked for system specific training and support for the DSL and IT staff as required;
- we will regularly check that our filtering system remains current by using the internet filter test tool created and hosted by South West Grid for Learning (swgfl.org.uk)

14. Filtering

For filtering to be effective, it should meet the needs of both pupils and staff and reflect specific use of technology whilst minimising potential harms. An active and well managed filtering system is an important part of providing a safe environment for pupils to learn.

Our filtering system:

- filters all internet feeds, including any backup connections;
- is age and ability appropriate for the users, and is suitable for our setting;
- handles multilingual web content, images, common misspellings and abbreviations;
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and blocks them;
- provides alerts when any web content has been blocked;

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as a member of SLT and/or the DSL.

Our filtering systems allow us to identify the:

- device name or ID, IP address, and where possible, the individual
- time and date of attempted access
- search term or content being blocked

The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be made aware of this procedure. If staff or pupils discover unsuitable sites, the URL will be reported to the school Digital technology lead who will then record the incident and escalate the concern as appropriate. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP.

In this school we use tools to provide an additional level of protection for users on top of the existing filtering service.

15. Monitoring

We will employ effective monitoring strategies that meet the safeguarding needs of our school. Whilst we recognise that no monitoring can be 100% effective, we will ensure that, as a minimum, our monitoring system covers the following content:

Content	Explanatory notes – content or communications that:
Illegal	Is illegal (e.g. Child abuse images and terrorist content). It is important that safeguards for illegal content cannot be disabled by the user.
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010.
Drugs/Substance abuse	Displays or promotes the illegal use of drugs or substances.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.
Gambling	Enables gambling.
Pornography	Displays sexual acts or explicit images.
Self-Harm	Promotes or displays deliberate self-harm (including suicide and eating disorders).
Violence	Displays or promotes the use of physical force intended to hurt or kill.
Suicide/self-harm	Suggest the user is considering suicide or self-harming.

Figure 3: Monitoring systems - inappropriate content (reproduced from UKSIC guidance)

In order to achieve this, the following arrangements will apply.

- We will follow the guidance set out for schools by the UK Safer Internet Centre on 'Appropriate Monitoring for Schools' to inform our monitoring strategy.
- The Governing Body will support the SLT to make sure effective device monitoring is in place which meets this standard and the risk profile of the school.
- the DSL will take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.
- Training will be provided to ensure that the specialist knowledge of both safeguarding and IT staff remains current.
- Staff will provide effective supervision, take steps to maintain awareness of how devices are being used by pupils/others and report any safeguarding concerns to the Head teacher.

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not prevent users from accessing material through internet searches or software.

Monitoring allows the school to review user activity on our devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action and record the outcome.

Our monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies are required to minimise safeguarding risks on internet connected devices and 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.

The Governing Body support SLT to review the effectiveness of our monitoring strategies and reporting process. We will always make sure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. It is clear to all staff how to deal with these incidents and who should lead on any actions.

Device monitoring is managed by the Head teacher/DSL and Securly they will:

- ensure monitoring systems are working as expected;
- provide reporting on pupil device activity at intervals to be determined by the school;
- receive safeguarding training including online safety;
- record and report safeguarding concerns to the DSL;

Those involved will also ensure that:

- monitoring data is received in a format that staff can understand;
- users are identifiable to the school, so concerns can be traced back to an individual, including guest accounts.

Where we make use of mobile or app technologies, then we will apply a technical monitoring system to the devices since the normal filtering system might not pick up mobile or app content. We will discuss this with our external provider

Our monitoring system will alert us to behaviours associated with the 4c's as outlined in Section 1 – Introduction – above.

16. Review of filtering and monitoring

The Governing body have overall strategic responsibility for meeting the standard which relates to the review of filtering and monitoring. They should make sure that filtering and monitoring provision is reviewed at least annually and may form part of a wider online safety review. Tools such as the SWGfL 360 degree safe self-review tool or the LGFL Online Safety Audit, will help to ensure that filtering and monitoring are working as expected across all devices, including mobile devices.

Reviews of filtering and monitoring are carried out to identify our current provision, any gaps, and the specific needs of any pupils and staff.

Prior to undertaking the review, we will consider the following:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL);
- what our filtering system currently blocks or allows and why;
- any outside safeguarding influences, such as county lines;
- any relevant safeguarding reports;
- the digital resilience of our pupils;
- teaching requirements, for example, our RHSE and PSHE curriculum;
- the specific use of our chosen technologies, including Bring Your Own Device (BYOD);
- the related safeguarding or technology Policies we already have in place;
- the checks that are currently taking place and how resulting actions are handled.

As a result, and to ensure it remains effective, our review of filtering and monitoring will inform:

- related safeguarding or technology policies and procedures;
- roles and responsibilities;
- any gaps in training for staff;
- curriculum and learning opportunities;
- procurement decisions;
- how often and what is checked;
- monitoring strategies.

Although the DfE standards recommended that the review of the filtering and monitoring systems is undertaken at least annually, we will also consider a review when:

- a safeguarding risk is identified;
- there is a change in working practice, like remote access or BOYD;
- new technology is introduced.

As part of the review process, there are a number of external tools which can be used to support the school:

- SWGfL 360 degree safe toolkit
- LGfL Safeguarding resources
- LGFL Online Safety Audit
- LGfL Safeguarding question bank for Governors (includes online safeguarding questions)
- UKCIS (UK Centre for Internet Safety) 'Questions from the governing board'
- UKCIS Online Safety Audit Tool for trainee and early career teachers
- UKCIS 'External visitors guidance'

The review is conducted by the Head teacher/DSL and the IT service provider and, where necessary the responsible governor will be involved. The results of the online safety review will be recorded on the SWGFL Filtering and Monitoring Checklist Register (or similar), actioned and shared with staff as appropriate and made available to those entitled to inspect that information.

Reviews may be conducted more frequently if a safeguarding risk is identified (as outlined above), or there is a change in working practice (e.g. remote access or BOYD) or if new technology is introduced. Changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the SLT. The outcomes from all filtering and monitoring reviews will be recorded.

We will undertake checks of our filtering provision the regularity of which will be based on the context, the risks highlighted in the filtering and monitoring review and any other risk assessments. Any checks will be undertaken from both a safeguarding and IT perspective. We can also make use of the South West Grid for Learning (SWGfL) filtering testing tool which checks that our filtering system is blocking access to illegal child sexual abuse material; unlawful terrorist content; and adult content.

When checking our filtering and monitoring systems, we will ensure that the system setup has not changed or been deactivated and the checks will include a range of:

- school owned devices and services (for both pupils and staff), including those used off site;
- implications in relation to geographical areas across the school site;
- user groups, e.g. teachers, pupils and guests.

Records will be held in the form of a System filtering and monitoring checks record/log so that they can be reviewed. Our record/log will include:

- when the checks took place;
- who did the check;
- what they tested or checked;
- resulting actions.

Checks (termly) might include any or all of the following:

- settings and updates on for example Google for Education and Microsoft systems;

- all in-school staff device password and log-on checks, including those which are used in the home environment;
- pupil and staff account compliance checks;
- maintenance of subscriptions and licences;
- revision and review of policies and procedures.

17. Reporting safeguarding and technical concerns

All staff are aware of the reporting mechanisms in place for reporting concerns about safeguarding and technical issues. Staff are advised to report if:

- they witness or suspect unsuitable material has been accessed;
- they can access unsuitable material;
- they are teaching topics which could create unusual activity on the filtering logs ;
- there is failure in the software or abuse of the system;
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks;
- they notice abbreviations or misspellings that allow access to restricted material.

18. Filtering and monitoring resource list / sources of further information

DfE Keeping children Safe in Education

DfE Broadband internet standards for schools and colleges

DfE Filtering & monitoring standards for schools and colleges

DfE Cyber security standards for schools and colleges

LGfL Free Training on Filtering and Monitoring

LGfL Online Safety Audit Toolkit

Smoothwall Benchmarking Your Digital Safeguarding - Strategies for Ofsted

SWGfL Filtering and Monitoring Checklist Register

SWGfL 360o Safe - Online safety review tool

UKSIC Guidance on Appropriate Filtering

UKSIC Guidance on Appropriate Monitoring

UKSIC Online safety in schools and colleges: Questions from the Governing Board 2022

UKSIC Webinar: Introduction to Filtering & Monitoring

UKSIC Webinar: Overview of Filtering & Monitoring Standards

UKSIC Webinar: Filtering & Monitoring Systems - Assessing Risk

UKSIC Webinar: Filtering & Monitoring Safeguards

UKSIC Webinar: Filtering & Monitoring Responsibilities & Documenting

ONLINE SAFETY LINKS

This list provides links to relevant government guidance and a range of national organisations who can offer support to schools.

Related guidance is available on:

- Relationships and sex education (RSE) and health education
- National curriculum in England: computing programmes of study
- National curriculum in England: citizenship programmes of study
- Generative artificial intelligence (AI) in education
- Using AI in education settings: support materials
- Generative AI: product safety expectations

Support and resources are also available from:

- National Centre for Computing Education (NCCE)
- UK Council for Internet Safety (UKCIS)
- UK Safer Internet Centre (UKSIC)
- Education for a Connected World
- CEOP (Child Exploitation and Online Protection Centre)
- CEOP Education Programme (Thinkuknow.co.uk)
- Cumberland Safeguarding Children Partnership (SCP)
- Information Commissioner (IC)
- Teaching online safety in schools
- The PREVENT Duty: an introduction for those with safeguarding responsibilities in schools
- How social media is used to encourage travel to Syria and Iraq: briefing note for schools – Home Office advice
- Internet Watch Foundation (IWF)
- Smoothwall

Schools can also get advice from national organisations such as:

- Anti-Bullying Alliance
- Association for Citizenship Teaching
- The Diana Award
- Hopes and Streams (survey report from LGfL)
- Internet Matters
- NSPCC learning
- Parent Zone's school resources
- PSHE Association
- SWGfL
- Better Internet for Kids
- We protect Global Alliance: Global Taskforce on child sexual abuse online - Report abuse
- Cyberbullying.org

You can refer parents to the following national organisations for support:

- Internet Matters
- NSPCC
- Parent Zone
- Facebook Advice to Parents
- Family Online Safety Institute (FOSI)
- Get safe online - Test your online safety skills

You can refer pupils to the following national organisations for support:

- BBC Own It
- Childline
- Childnet