





Online Safety Policy & Procedures

Including the school's 'Bring your own device – (BYOD) Policy' and 'ICT Acceptable Use Agreements'

Approved by		
Name:	Clem Coady	Steve Cook
Position:	Head Teacher	Chair of Governors
Signed:		
Date:	17 June 2024	
Proposed review date:	16 June 2025 (Statutory annual review)	

'Living and learning together to care for each other and our world.'

KEY ROLES

The following key roles were held as at the date of publication:

<ul style="list-style-type: none"> • Designated Safeguarding Lead (DSL) – which also encompasses the role of Online Safety Lead • Remote Education Lead • Network Manager • Data Protection Officer (DPO) 	Clem Coady – Head teacher
<ul style="list-style-type: none"> • Computing Subject Lead 	Clem Coady and Bernadette Cook (Computing Specialist Teacher)
<ul style="list-style-type: none"> • Deputy Designated Safeguarding Leads (DDSL) 	Wendy Pratt and James Webb
<ul style="list-style-type: none"> • PSHE Lead • Relationships Education, Sex Education & Health Education Lead 	Clem Coady and James Webb
<ul style="list-style-type: none"> • Chair of Governors 	Steve Cook
<ul style="list-style-type: none"> • Online Safety / Safeguarding Link Governor 	Phil Askew
<ul style="list-style-type: none"> • IT Service/Support Provider 	Gemini IT
<ul style="list-style-type: none"> • Website Host 	Wix
<ul style="list-style-type: none"> • The school's information systems (broadband / system security / online suppliers / anti-virus protection / online filtering services) are organised by: 	The Local Authority(*)

(*) The online filtering services provided by the LA are under review, and may change.

REVIEW SHEET

Each entry in the table below summarises the changes made to this document since the last review.

Version Number	Version Description	Date of Revision
01	Original. Rewritten to take into account current national guidance on Online Safety	Nov 2019
02	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. Minor policy addition to draw attention to policy or procedure addendums staff and others must be aware of (usually Covid-19 related). Minor policy clarification in section on BYOD procedures to specifically reference wearable technologies and the broadcasting of location data.	Sept 2020
03	Updated to include additional information on sharing nude and semi-nude images and online challenges and hoaxes.	Mar 2021
04	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 will provide remote education and do it safely. Minor updates to appendices to reflect language/KCSiE updates.	Sept 2021
05	Updated in line with statutory DfE guidance 'Keeping Children Safe in Education' Sept 2022. Changed BYOD into a specific section to make it easier to find and reference. 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
06	Reviewed and personalised for our School. Note: ICT Acceptable Use Agreements for 'Pupil/Parent' and 'Staff/Volunteer/Governor' have been updated 28/04/23	02/05/2023
07 / 08	Updated in line with KCSiE 2023 (filtering and monitoring) and to various links	Sept 2023
	KAHSC filtering and monitoring guidance is now shown as Appendix A and provides specific detail on how the school will manage filtering and monitoring of the technology used and of school-owned devices.	Nov 2023
	Minor updates with links to DfE guidance for schools on creating a Mobile Phone Policy/procedure for pupils.	Feb 2024
	Policy & ICT Acceptable Use Agreements updated.	01/04/2024
09	Policy & ICT Acceptable Use Agreements updated.	17/06/2024

TABLE OF CONTENTS

KEY ROLES	1
REVIEW SHEET	2
TABLE OF CONTENTS	3
POLICY AND PROCEDURES	5
1. Definitions	5
2. Introduction to online safety in our school	5
3. Background/Rationale	5
4. Communication & monitoring of this Policy and procedures	6
5. Scope of the Policy	6
6. Roles and Responsibilities	7
6.1 Governors	7
6.2 Head teacher	8
<i>The Head teacher's role/responsibilities for Online Safety as Head teacher of the School:</i>	<i>9</i>
<i>The Head teacher's role/responsibilities for Online Safety as Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL)</i>	<i>10</i>
<i>The Head teacher's role/responsibilities for Online Safety as Computing Subject Lead</i>	<i>11</i>
<i>The Head teacher's role/responsibilities for Online Safety as Network Manager</i>	<i>11</i>
<i>The Head teacher's role/responsibilities for Online Safety as Data Protection Officer (DPO)</i>	<i>12</i>
6.3 PSHE Lead; and Relationship Education, Sex Education & Health Education Lead	13
6.4 All Staff	13
6.5 Volunteers and contractors	14
6.6 Pupils	14
6.7 Parents	15
7. Teaching and Learning	16
7.1 Online resources used in our School to enhance learning	16
7.2 Four areas of online safety risk – “The 4 Cs”	16
7.3 Internet safety through the curriculum	16
7.4 How internet use enhances learning	17
7.5 Pupils with additional needs	17
7.6 Remote Education	18
8. Flowchart – Response to an Online Safety Incident or Concern	21
9. Handling online safety concerns and incidents	22
9.1 Sharing nude and/or semi-nude images and/or videos	23
9.2 Upskirting	24
9.3 Cyberbullying	24
9.4 Harmful online challenges or hoaxes	25
9.5 Sexual violence and harassment	26
9.6 Misuse of school technology (devices, systems, networks, or platforms)	26
9.7 Social media incidents	27
10. Data protection and data security	27
10.1 Maintaining Information Systems Security	28
10.2 Password Security	28
<i>Training/Awareness regarding Password security:</i>	<i>28</i>
10.3 Audit/Monitoring/Reporting/Review of data security	29
11. Electronic Communications	29
11.1 Email	29
11.2 Emailing personal, sensitive, confidential, or classified information	30
11.3 Zombie accounts	30
12. School Website	30

13. Use of digital and video images.....	30
14. Cloud Platforms	32
15. Social Media, social networking & personal publishing sites.....	32
15.1 The School's Social Media.....	32
15.2 Staff, pupils', and parents' Social Media presence	33
16. Personal devices and bring your own device (BYOD) procedures:.....	34
16.1 Searching, Screening and Confiscation	36
17. Managing filtering and monitoring.....	36
18. Policy Decisions	37
18.1 Authorising internet access.....	37
18.2 Assessing risks.....	37
18.3 Responding to incidents of concern.....	38
19. Communicating Policy and procedures	38
19.1 Introducing the online safety Policy and procedures to Pupils	38
19.2 Discussing the Policy and procedures with staff, volunteers & governors	38
19.3 Parents and the online-safety policy.....	39
20. Complaints.....	40
21. Associated School Policies and procedures	41
ONLINE SAFETY GUIDANCE AND LINKS	41
APPENDIX A – ONLINE SAFETY – FILTERING AND MONITORING ARRANGEMENTS	42
1. Introduction.....	42
2. DfE Filtering and monitoring standards	43
3. Blocking harmful and inappropriate content	45
4. Filtering	46
5. Monitoring	46
6. Review of filtering and monitoring.....	48
7. Reporting safeguarding and technical concerns.....	50
8. Filtering and monitoring resource list / sources of further information	50
FILTERING AND MONITORING CHECKS - RECORD SHEET	51
1. System checks - Filtering system.....	51
2. System checks - Monitoring system.....	52
LEGAL FRAMEWORK	53
ICT ACCEPTABLE USE AGREEMENT – PUPIL/PARENT	58
ICT ACCEPTABLE USE AGREEMENT – STAFF/VOLUNTEER/GOVERNOR	60

POLICY AND PROCEDURES

1. Definitions

For the purposes of this Policy and procedures 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.

The term 'school' refers to Stoneraise School. The term 'school' also includes wrap around care, such as Breakfast Clubs and After School Clubs.

'ICT' means Information and Communication Technologies.

2. Introduction to online safety in our school

Staying safe online is a concern for all children and parents. We live in an age where technology is an integral part of life. With its use comes tremendous advantages but it also has its challenges.

Knowing the potential threats and how to deal with them are a skill set needed by everyone. At our school we achieve this through our curriculum and through discussions with children/staff/volunteers/governors and parents. We encourage an open culture where children feel safe to discuss their online activity.

3. Background/Rationale

New technologies have become integral to the lives of children and young people in society, both in school and in their lives 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 and young people 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. This Online Safety Policy and procedures will help to ensure safe and appropriate use, and the development and implementation will involve the Head teacher, Governors, teachers, other staff, parents, and pupils.

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 young people 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 exploitation;
- The sharing/distribution of personal images 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 prejudiced-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, 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.

As a school we aim to provide the necessary safeguards, and do everything that could reasonably be expected of us to manage and reduce these risks. This Online Safety Policy and procedures 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.

4. Communication & monitoring of this Policy and procedures

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

- Posting it on the school website, and making paper copies available on request from the school office;
- Discussing school policy and procedures during induction/entry with new staff/volunteers/governors, and using the [ICT Acceptable Use Agreement - Staff/Volunteer/Governor](#);
- Ensuring new pupils to school are presented with an ICT Acceptable Use Agreement.
- Discussing online safety rules with pupils and using the [ICT Acceptable Use Agreement - Pupil/Parent](#);
- Holding ICT Acceptable Use Agreements in pupil and personnel files (part of the Welcome Pack).

The Online Safety Policy is also referenced in other school Policies and procedures as outlined in the section below titled [Associated School Policies and procedures](#).

5. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, 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. This includes incidents of cyberbullying, 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 2011 Education Act 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 such incidents within this Policy and procedures and the 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.

6. Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety within the school. See also the table above titled [Key roles](#).

6.1 Governors

The role of the Governors and the Online Safety Governor is to:

- ensure a member of the Governing Body is elected to the role of Online Safety Governor, who should then lead on the relevant governance requirements outlined below;
- ensure that the Head teacher (or an alternative senior member of staff) is appointed to the following roles, and ensure they are given the appropriate status, authority, time, funding, training, resources, and support;
 - Designated Safeguarding Lead (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);
 - Remote Education Lead
 - Computing Subject Lead;
 - Network Manager;
 - Data Protection Officer
 - Deputy Designated Safeguarding Lead;
 - PSHE Lead;
 - Relationship Education, Sex Education & Health Education Lead;
- 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 receiving regular information about online safety incidents and monitoring reports;
- make use of the UK Council for Internet Safety (UKCIS) guide audit tool on at least an annual basis: [Online safety in schools and colleges: Questions from the Governing Board](#);
- ensure that appropriate filters and appropriate 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 Head teacher 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;
- ensure that the school follows current online safety advice (including that for online filtering and monitoring) to keep both pupils and staff safe;
- support the school in encouraging parents and the wider school community to become engaged in online safety activities;
- have regular reviews with the Head teacher (in their capacity as Online Safety Lead/Designated Safeguarding Lead), and incorporate online safety into standing discussions of safeguarding at Governors meetings (including incident logs, adverse monitoring reports, change control logs etc);
- ensure that where the online safety coordinator is not the named DSL or deputy DSL, there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety as a whole is not compromised;
- work with the 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 outlined in Annex B of '[Keeping Children Safe in Education](#)' which contains important additional information about specific forms of abuse and safeguarding issues;
- ensure that all staff undertake regular updated safeguarding training, including online safety training in line with advice from the Local Safeguarding Children's Partnerships (LSCP), and that it is integrated, aligned, and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning; (See the section titled [training](#) below.)
- ensure that appropriate filters and appropriate 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 Head teacher and relevant staff have an awareness and understanding of the provisions in place to manage filtering and monitoring and how to escalate concerns when identified;
- 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;
- ensure that there is an audit system in place to monitor the Head teacher's work (in their capacity as Network Manager), carrying out internal technical online safety procedures.

6.2 Head teacher

In our school the Head teacher has overall responsibility, and day-to-day responsibility, for online safety provision. The Head teacher also holds the following supplementary roles/responsibilities:

- [Designated Safeguarding Lead \(DSL\) with lead responsibility for safeguarding and child protection, and overarching responsibility as Online Safety Lead;](#)
- [Computing Subject Lead;](#)
- [Network Manager;](#)

- [Data Protection Officer](#).

Each of the above roles is expanded upon in the following section:

The Head teacher's role/responsibilities for Online Safety as Head teacher of the School:

- To take overall responsibility for data and data security;
- To foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding;
- To ensure that Policies and procedures are followed by all staff and other adults working paid or unpaid in the school;
- To 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](#).
- To be aware of all online-safety issues which might arise, and keep abreast of school issues and broader policy and practice information;
- To take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling;
- To work with the Governors to ensure a Data Protection Act 2018 (DPA) compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information;
- To ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles;
- To 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 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;
- To 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 – Response to an Online Safety Incident or Concern](#);
- encourage parents/carers 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/carers will be regularly updated and published on the school website and via newsletters and other publications.
- To 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.

- To ensure that there is an audit system in place to monitor and support staff that carry out internal technical online safety procedures;
- To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety;
- To ensure the school website meets statutory requirements; and
- All of the responsibilities listed in the '[all staff](#)' section below.

The Head teacher's role/responsibilities for Online Safety as Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL)

In our school the Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL) is the Head teacher. As outlined in [Keeping Children Safe in Education](#) the Designated Safeguarding Lead/Online Safety Lead will:

- take lead responsibility for safeguarding and child protection (including online safety 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 nude and/or semi-nude images and/or videos/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 approach to online safety 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;
- liaise with other agencies in line with '[Working together to Safeguard Children](#)' statutory guidance;
- have an understanding of the unique risks associated with online safety (including an understanding of the filtering and monitoring systems and processes in place in the school) 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;
- take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns;
- 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 Governors 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., ICT 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, including external bodies such as the IT Service/Support Provider;
- communicate regularly with the designated online safety Governor 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 sexual violence and sexual harassment (Part five - [Keeping Children Safe in Education](#)) 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 read and understand [KCSiE Part one](#) (which includes Annex B). The DSL/Head teacher and Deputy DSL must read and understand the whole of [Keeping Children Safe in Education](#)
 - all staff are aware of information relevant to their role in keeping children safe online signposted in KCSiE [Annex B](#)
 - cascade knowledge of risks and opportunities 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;
 - access to illegal/inappropriate materials;
 - inappropriate online contact with adults/strangers;
 - potential or actual incidents of grooming;
 - cyberbullying and the use of social media.
 - keep abreast of current issues and guidance through organisations such as [CEOP](#) and [Think U Know](#)

The Head teacher's role/responsibilities for Online Safety as Computing Subject Lead

In our school the Computing Lead is the Head teacher along with a computing specialist teacher. Their responsibilities include:

- the overseeing delivery of the online safety element of the Computing curriculum in accordance with the national curriculum;
- working closely with all other staff to ensure an understanding of the issues, approaches, and messages within Computing; and
- collaborating with internal and external support staff/contractors responsible for ICT use in school to ensure a common and consistent approach, in line with ICT Acceptable Use Agreements.

The Head teacher's role/responsibilities for Online Safety as Network Manager

In our school the Network Manager is the Head teacher. Their responsibilities include:

- to ensure that the school's IT support/service provider carries out all the online safety measures that would otherwise be the responsibility of the school's technical staff, as suggested below;
- to ensure that school's IT support/service provider is fully aware of the Online Safety Policy and associated procedures;
- supporting Governors and the school in achieving the DfE [digital and technology standards](#);
- supporting the school 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;
- keeping up to date with technical information and this Policy to effectively carry out their online safety role and to inform and update others as relevant;
- ensure that school systems and networks reflect school Policy, and where necessary work with others in the achievement of this;
- ensuring that relevant 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 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;
- ensure the school website meets statutory DfE requirements;
- reporting online safety issues that come to their attention in line with school Policy.

The Head teacher's role/responsibilities for Online Safety as Data Protection Officer (DPO)

In our school the Data Protection Officer (DPO) is the Head teacher. Their responsibilities include:

- to be familiar with references to the relationship between data protection and safeguarding outlined in key DfE documents '[Keeping Children Safe in Education](#)' and '[Data protection: a toolkit for schools](#)'.
- to understand that:
 - Neither the Data Protection Act 2018 nor UK GDPR 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, 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 the need to safeguard and promote the welfare of children.
 - As with all data sharing, appropriate organisational and technical safeguards will be in place.

- work with the 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.

6.3 PSHE Lead; and Relationship Education, Sex Education & Health Education Lead

In our school the PSHE Lead, and the Relationship Education, Sex Education and Health Education Lead is a senior teacher who is named in the section above titled [Key roles](#). Their responsibilities include:

- all of the responsibilities listed in the '[all staff](#)' section below;
- ensuring that consent, mental wellbeing, healthy relationships and staying safe online is embedded into the PSHE, relationships education, sex education 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 and all other staff to ensure an understanding of the issues, approaches, and messages within PSHE, relationships education, sex education and health education.

6.4 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 that it is the Head teacher that undertakes the role of Designated Safeguarding Lead and Online Safety Lead in our school;
- read and understand [Part one \(which includes Annex B\)](#) of '[Keeping Children Safe in Education](#)' (unless they **do not** work directly with children when they must read and understand Annex A instead);
- 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 [ICT Acceptable Use Agreement for staff/volunteers/governors](#);
- be aware of online safety issues related to the use of mobile technology e.g., phones, cameras and other hand-held devices and follow school procedures in relation to these devices – see the section titled [Personal devices and bring your own device \(BYOD\) procedures](#);
- 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;

- 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 in accordance with school procedures;
- notify the DSL 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 augmented reality, 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;
- 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 law;
- prepare and check all online source and resources before using in the classroom;
- encourage pupils to follow their ICT 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 bullying and low-level sexual harassment either offline or online;
- 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.

6.5 Volunteers and contractors

The key responsibilities of volunteers and contractors are to:

- read, understand, sign, and adhere to the [ICT Acceptable Use Agreement for staff/volunteers/governors](#);
- report any concerns, no matter how small, to the DSL without delay;
- maintain an awareness of current online safety issues and guidance;
- model safe, responsible, and professional behaviours in their own use of technology.

6.6 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 [ICT Acceptable Use Agreement - Pupil/Parent](#), which they and their parents will be expected to sign before being given access to school systems. As with consent on data (privacy notices)

Agreements must be written in terms the EYFS/KS1 child can understand; **(NB. at EYFS and KS1 parents can sign on behalf of the pupils but pupils must understand the Agreement)**

- 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 online 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 ICT 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, hand-held digital devices, and other digital devices – see the section titled [Personal devices and bring your own device \(BYOD\) procedures](#);
- know and understand school procedures on the taking/use of images and on cyberbullying/sharing nude and/or semi-nude images and/or videos;
- 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.

6.7 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 therefore 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 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 [ICT Acceptable Use Agreement – Pupil/Parent](#) 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.

7. Teaching and Learning

7.1 Online resources used in our School to enhance learning

All pupils have an iPad each with uses Apple Classroom for teachers to monitor their on-screen activity. Profiles are in place which filter content and restrict children from deleting web history.

7.2 Four areas of online safety risk – “The 4 Cs”

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, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; 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:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (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.

7.3 Internet safety through the curriculum

Strong links between teaching online safety and the curriculum are the clearest in:

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

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 leaders 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 augmented reality, 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), 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.

7.4 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:
 - search safely online – through e.g. Search Coach;
 - 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;
 - 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;
 - understand why and how some people will 'groom' young people for sexual or extremist ideology reasons;
 - understand the impact of cyberbullying, sharing inappropriate images 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 ICT 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.

7.5 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.

We will:

- 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.
- Use Search Coach & the ICT Acceptable Use Agreement to help pupils transfer online safety rules to other lessons and environments.
- 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.)
- Provide 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.
- Apply consistent use of cause and effect, linking the rules to consequences, teaching realistic and practical examples of 'what might happen if...' without frightening pupils.

7.6 Remote Education

Expired legislation which led to the [Remote Education \(England\) Temporary Continuity \(No.2\) direction](#) no longer has effect, but 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.

In these circumstances pupils will have access to remote education as soon as we reasonably can in proportion to the length of absence and disruption to their learning.

We will try to provide remote education equivalent in length to the core teaching pupils would receive in school. This can include recorded or live direct teaching time, as well as time for pupils to complete tasks and assignments independently, and we understand good practice is considered to be:

- 3 hours a day on average across the cohort for key stage 1, with less for younger children
- 4 hours a day for key stage 2

In developing our remote education provision, we have:

- Decided that the Head teacher will take overarching responsibility for the oversight of the quality, delivery, and safety of remote education.
- selected the Microsoft Teams digital platform to use consistently across the school to allow interaction, assessment, and feedback with procedures in place to ensure staff are trained and confident in its use. This enables us to provide online video lessons recorded

by teaching staff and high-quality lessons developed by external providers as well as monitored methods of communication.

- identified ways to discover and overcome barriers to digital access for pupils e.g., forms or other survey methods, distributing school-owned laptops, securing appropriate internet connectivity solutions, providing printed resources, such as textbooks and workbooks, to structure learning, supplemented with other forms of communication to keep pupils on track or answer questions about work.
- ensured that school-owned devices distributed for the purpose of access to remote education will always include appropriate safeguarding controls and support to help children and families, and staff use them safely, including information about physically healthy computing e.g. posture, the teaching and learning environment, and the importance of sleep.
- Considered how to transfer effective teaching from the classroom into remote education.
- Determined our thresholds of absence at which we will again publish (on the school website) up-to-date [information](#) about what is intending to be taught and practised in each subject so that pupils can progress through the curriculum. This may trigger reviews and updates of relevant Policies, procedures, and supporting documents such as our ICT Acceptable Use Agreements.
- Put systems in place for checking, daily, whether pupils are engaging with their work, so we can work with families to rapidly identify effective solutions where engagement is a concern.
- Considered issues that specific individuals or groups of pupils may have engaging with remote education due to their age, stage of development, special educational needs, or disability e.g., where this would place significant demands on parents' help or support, ensuring that the teachers best placed to know how the pupil's needs can be most effectively met to ensure they continue to make progress, work with families to deliver an ambitious and appropriate curriculum
- Sought to demonstrate that we understand the requirement for schools under the [Children and Families Act 2014](#) to use our best endeavours to secure the special educational provision called for by the pupils' special educational needs remains in place.
- Identified potential personal, professional, and children's safeguarding issues associated with the provision of remote education; put in place hardware, software, procedures, and training to reduce the risk of harm to the adults, children, and young people exposed to it; and ensured the risks are being addressed in a consistent and ongoing way through the curriculum (see below).

In the provision of remote education this school undertakes to:

- Communicate with parents to reinforce the importance of children being safe online by providing information on the systems we use to filter and monitor online use
- Set meaningful and ambitious work each day in an appropriate range of subjects, with clear information for parents on what their child is being asked to do online (including the sites they will be asked to access), and who from the school their child is going to be interacting with online
- Transfer into remote education what we already know about effective teaching in live classrooms by:
 - providing frequent, clear explanations of new content, delivered by a teacher or through high-quality curriculum resources
 - providing opportunities for interactivity, including questioning, eliciting and reflective discussion
 - providing scaffolded practice and opportunities to apply new knowledge

- enabling pupils to receive timely and frequent feedback on how to progress, using digitally facilitated or whole-class feedback where appropriate
- using assessment to ensure teaching is responsive to pupils' needs and addresses any critical gaps in pupils' knowledge
- avoiding an over-reliance on long-term projects or internet research activities
- Ensure teachers can access the DfE webpage [Get help with technology for remote education](#) which signposts to Microsoft etc. guidance on setting up devices for remote learning safely.
- Review and self-assess our remote education offer regularly.
- Continue to record attendance accurately in the register for pupils who are receiving remote education in line with DfE non-statutory guidance [Working together to improve school attendance](#).
- Carry out an annual review of the school's approach to online safety, supported by an [annual risk assessment](#) that considers and reflects the risks the pupils that attend this school face using a tool like the [360 safe website](#).

We recognise that there are additional safeguarding risks to pupils associated with them spending more time online, both in their leisure time and to be able to access remote education. There may also be risks from or to the people they live with during live video link work and staff are expected to plan accordingly and seek advice from the DSL as necessary. The pupil ICT Acceptable Use Agreement includes expected conduct during remote education activities.

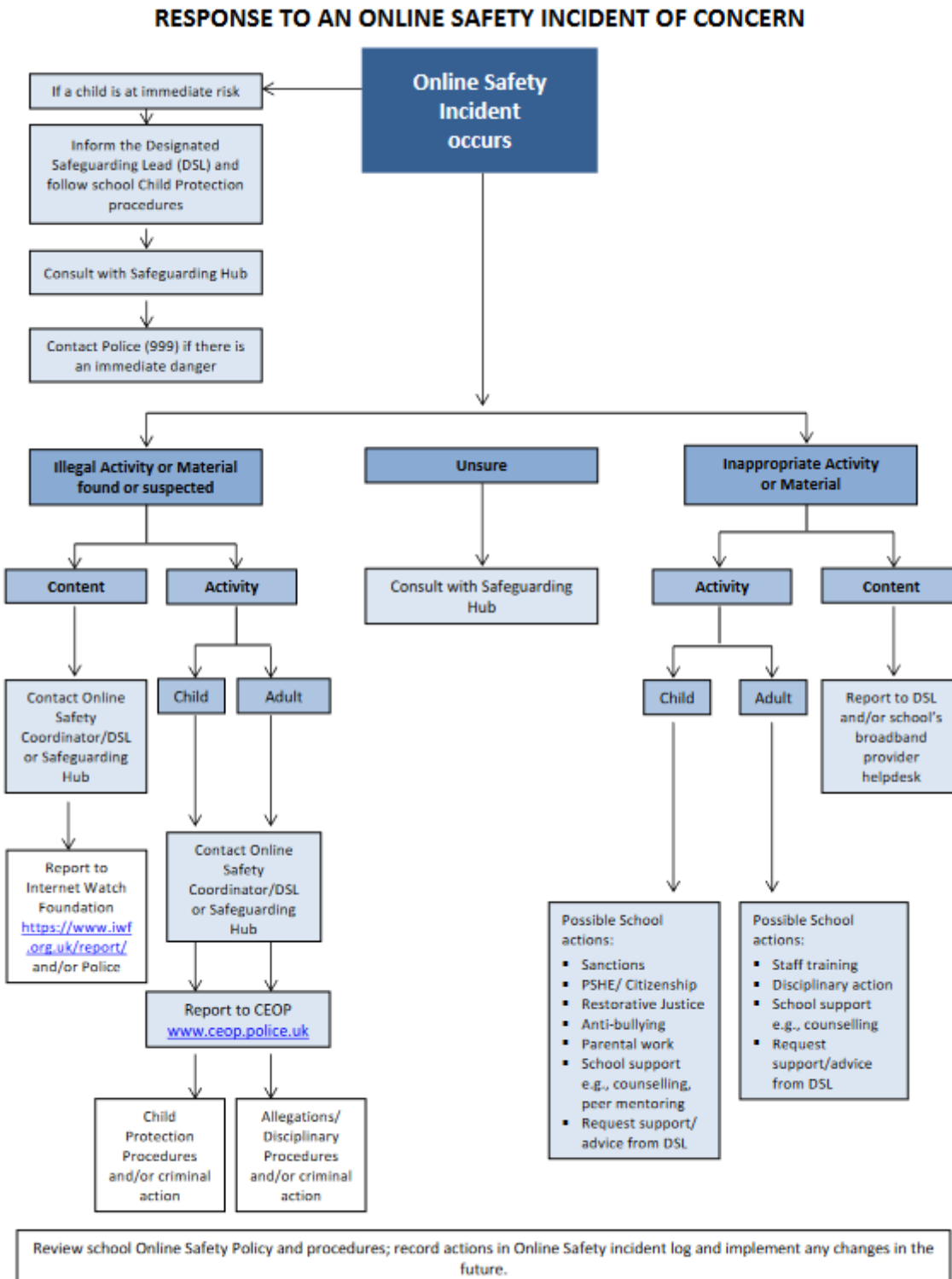
We recognise that there are additional safeguarding risks to staff as well, especially those facilitating remote learning via live video links that may also impact other people in their household or community.

Staff are expected to:

- follow DfE guidance [Safeguarding and remote education](#) and safeguarding procedures when planning remote education strategies and teaching remotely
- Provide information about their temporary home working environment insofar as it might impact on their physical health, or the safeguarding of learners or their own household.
- Act appropriately on feedback and use any necessary online or cyber tools provided.
- Provide information about the technology they use at home to get online i.e., to ensure compatibility with school systems, especially cyber security measures involved in accessing sensitive data like medical, behaviour or performance information on school servers remotely.
- Implement relevant guidance on safe teaching and pastoral care from their home e.g., what is in the background of recorded or live streams, what is visible on shared screens, what can be heard by others in a household etc.
- Pay special attention to how they protect personal data at home.
- Report to the Head teacher any issues or concerns they may have either about their personal safety or that of a pupil.
- Keep talking about staying safe online, which we can do by:
 - Ensuring staff have the tools to promote a healthy balance between the positive and negative aspects of life online.
 - Signposting parents to tools to explain and reduce risks and help them talk to their child.
 - Reiterating behaviour expectations and ways to handle and report problems, especially encouraging children to speak to a trusted adult if they come across content online that makes them uncomfortable.

- o Supporting critical thinking and promoting resources like [It's not easy being a parent in the digital age | Parent Zone](#) which provide ways parents can help their child develop these skills.

8. Flowchart – Response to an Online Safety Incident or Concern



KAHSC – V2 September 2023

9. 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; Relationships Education, Sex Education and Health Education; 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/documents:

- Child Protection Policy and procedures
- Behaviour Policy and procedures (includes anti-bullying procedures)
- ICT Acceptable Use Agreements
- Data Protection Policy, agreements, and other documentation (e.g., privacy statement, consent forms for data sharing image use etc.)
- Prevent Risk Assessment

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 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., Local Authority Safeguarding Hub, UK Safer Internet Centre's Professionals' Online Safety Helpline (0344 3814772), 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 the sections below for procedures for dealing with the [sharing of nude and/or semi-nude images and/or videos](#), [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 Online Safety Lead will record all reported incidents, and actions taken, in the School Online Safety incident log and in any other relevant areas e.g., Bullying or Child protection log, ScholarPack system etc.

- The Designated Safeguarding Lead 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 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.
- 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 then the school will contact the Safeguarding Hub **and** escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub – see Child Protection Policy and procedures.

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. **Any such suspicion should be brought to the attention of the DSL, who will then direct further action and any possible investigation. Staff should not conduct investigations unless asked to do so by the DSL.**

(The DSL may ask more than one member of staff to be involved in an investigation, and ask for this to 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’, and the Head teacher will determine the information that can & cannot be communicated – e.g. the outcome of any disciplinary process would not be divulged.

9.1 Sharing nude and/or semi-nude images and/or videos

Where incidents of the sharing of nude and semi-nude images 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.

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 nude and semi-nude images 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 and young people;
- handling devices and images;
- recording incidents, including the role of other agencies.
- informing parents and carers

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.

9.2 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.

9.3 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 young people 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 young people, 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 feel 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, ICT 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.

9.4 Harmful online challenges or hoaxes

An online challenge will generally involve users recording themselves taking a challenge and then distributing the resulting images/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 the DSL. 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 school-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](#)'

9.5 Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Part five of '[Keeping Children Safe in Education](#)'. All staff are aware of this guidance.

We have a zero tolerance approach to all forms of sexual violence and harassment and will act appropriately on information which suggests inappropriate behaviour regardless of the considered seriousness. Any incident of 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.

9.6 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 ICT 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 in line with 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.

9.7 Social media incidents

See also the section titled [Social Media](#) below.

Social media incidents are governed by ICT Acceptable Use Agreements. Breaches will be dealt with in line with these procedures, the Behaviour Policy and procedures / 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 be 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](#) 'POSH' (UK Safer Internet Centre) for support or assistance in accelerating the process of removal.

10. 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 – this can be obtained from the school website, or on request from the school office.

There are references to the relationship between data protection and safeguarding in key DfE documents i.e. '[Keeping Children Safe in Education](#)' and '[Data protection: a toolkit for schools](#)' which the DPO/DSL will seek to apply.

The Head teacher and Governors will 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.

Note: Neither the Data Protection Act 2018 nor UK GDPR 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 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.

10.1 Maintaining Information Systems Security

The school's information systems (broadband / system security / online suppliers / anti-virus protection) are organised, as shown in the section above titled [Key roles](#).

The 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.

Local Area Network (LAN) security issues include:

- Users must act reasonably e.g., the downloading of large files or viewing 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 ICT 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 the Headteacher and our network provider.

10.2 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.

- Adult users are provided with an individual network username and password, and email address (if required).
- All members of staff are aware of the dangers inherent in leaving ScholarPack (Data Management System), for pupil-tracking and digital registers, open and of the importance of keeping passwords secret.
- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Training/Awareness regarding Password security:

Users will be 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 ICT Acceptable Use Agreement.

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

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

10.3 Audit/Monitoring/Reporting/Review of data security

The Head teacher 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](#).

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 the Online Safety Lead and Online Safety Governor at regular intervals.

11. Electronic Communications

11.1 Email

Our general principles for email use are as follows:

- Staff will only use official school provided email accounts to communicate with pupils and parents. 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 Head teacher.
- Pupils and staff are 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.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Users must immediately report to the 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.

11.2 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;

11.3 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.

Staff will refer to further advice available at [IT Governance](#) as necessary.

12. School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Head teacher 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 host is shown in the section titled [Key Roles](#) above.

The DfE has determined information which must be available on a school website. '[What maintained schools must publish online](#)' which the school adheres to.

The school follows these principles:

- The contact details on the website are the school address, email, and telephone number.
- Staff, Governors, or pupils' personal information are not published on the school website.
- 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. Full names are not published, and will not be included/saved within the file names/image names.

13. 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 will gain written permission from parents for the use (*) of digital photographs or video involving their child as part of the school's Admissions Form which the parent completes when their child joins the school. This consent is considered valid for the entire period that the child attends this school. **(Parents may withdraw permission, in writing, at any time.)**
 - (*) The term 'use' can be taken to mean publication of the digital photograph/video image(s) on the school website/Twitter/Facebook posts.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- 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 full names 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.
- 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, and sign the school's ICT 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.
- 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.
 - In the event of parents wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc.
- 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 the school can refer to Kym Allan Health and Safety Consultants' (KAHSC) 'General Safety Series G21 – The use of images when working with children', and their 'Model consent form – trips, images and pain relief'.)
- A pupil's work can only be published, by the school, and/or by external agencies, with the consent of the pupil and parents.

14. Cloud Platforms

This school adheres to the principles of the DfE document '[Cloud computing services: guidance for school leaders, school staff and governing bodies](#)' and 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 Head teacher 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 Head teacher 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.
- Pupil images/videos are only made public with parental consent.
- Only school-approved platforms are used by students or staff to store pupil work.

15. Social Media, social networking & personal publishing sites

15.1 The School's Social Media

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 Instagram 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 and Text are the official electronic communication channels between parents and the school.
- Google Classroom is used between staff and pupils.
- Staff members communicate with each other using email, and our governors do the same.

15.2 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 ICT 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, students 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's Concerns and Complaints Policy and Procedures (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, or abuse. 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 (*) to be 'friends' with or make a 'friend request' (**) to any member of staff, governor, volunteer or regular school contractor or otherwise communicate via social media. Pupils are also discouraged from 'following' members of staff, governors, volunteers, or regular school contractor's 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.

() 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.*

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

Staff members 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 over-sharing 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.
- 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, 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 Head teacher before using Social Media tools in the classroom.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- 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's [ICT Acceptable Use Agreement - Staff / Volunteer / Governor](#).
- The school will be able to seek further guidance, as needed from the document filed 'Safe Use of Facebook and Other Social Networking Sites' which can be obtained by the Head teacher from the school's H&S Advisor (KAHSC).

16. Personal devices and bring your own device (BYOD) procedures:

We recognise that 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 (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 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 ICT Acceptable Use Agreement and Behaviour Policy and procedures.
- 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. The DSL will be consulted before any such search is carried out. Staff mobiles or handheld 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 school's Mobile phone procedures/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.

Mobile Phone Procedures:

- Mobile phones and personal devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. They should be switched off (not placed on silent) and stored out of sight on arrival at school. 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.
- 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.
- Mobile phones and personal devices are not permitted to be used in certain areas such as changing rooms, toilets, and swimming pools.

16.1 Searching, Screening and Confiscation

In line with the DfE guidance '[Screening, searching and confiscation: advice 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 of a child and/or video, 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.

17. Managing filtering and monitoring

For specific information on how we manage filtering and monitoring in our 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, Head teacher 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 will regularly review their effectiveness.

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](#) which set out that schools should:

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

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.

The following issues will be addressed and regularly reviewed in relation to the management of filtering:

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with the School's Broadband team to ensure that filtering procedures are continually reviewed.
- The school will have a clear procedure for monitoring and subsequent reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the Online Safety Lead/DSL who will then record the incident and escalate the concern as appropriate.
- The school filtering system will block all sites on the [Internet Watch Foundation](#) (IWF) list.

- Changes to the school filtering procedures will be risk assessed by the Head teacher.
- The Head teacher will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as [IWF](#), the Police or [CEOP](#).
- The school's access strategy will be designed by the Head teacher to suit the age and curriculum requirements of the pupils.

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).

18. Policy Decisions

18.1 Authorising internet access

The Network Manager 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 Network Manager 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 ICT Acceptable Use Agreement before using any school ICT resources.
- Parents will be asked to read and sign the School ICT 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 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.

18.2 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. The school will need to address the fact that it is not possible to completely remove the risk that pupils might access unsuitable materials via the school system.

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 by the Head teacher and teaching staff.

18.3 Responding to incidents of concern

Refer to the section titled [Handling online safety concerns and incidents](#) above.

19. Communicating Policy and procedures

19.1 Introducing the online safety 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 and 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.

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, and/or ICT programmes covering both safe school and home use.
- 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.

19.2 Discussing the Policy and procedures with staff, volunteers & governors

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.

All members of staff receive regular information and training on online-safety issues through the Online Safety Lead at staff meetings.

All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online-safety and know what to do in the event of misuse of technology by any member of the school community.

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, should discuss this with the Head teacher. Where concerns are related to children's safeguarding, they should be reported to the DSL (or Deputy 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.

A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use, both in and out of school.

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 confirm reading through Google Forms, relevant ICT Acceptable Use Agreements.
- For staff who manage filtering systems or monitor ICT use: that they will be supervised by the Head teacher, 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 school into disrepute, or if something is felt to have undermined confidence in their professional abilities.

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

19.3 Parents and the online-safety policy

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;
- encourage a partnership approach to online safety at home and at school which may include demonstration sessions, 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 ICT Acceptable Use Agreement for pupils and discuss its implications with their children and offer support to do this if required;
- provide information and guidance for families about 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 ICT Acceptable Use Agreement and if they understand the rules.

Parents are also required to make a decision as to whether they consent to images of their child being taken/used on the school website and Instagram.

20. 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.

- Concerns or complaints about the misuse of online systems will be dealt with under the school's Concerns and complaints procedure. These will always be notified to the Online Safety Lead.
- Complaints about cyberbullying are dealt with in accordance with our Anti-bullying procedures which form part of our Behaviour Policy and procedures.
- Concerns or 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 (any complaint about the Head teacher will be referred to the Chair of Governors).
- 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;
- referral to the Police.

21. Associated School Policies and procedures

This Policy should be read in conjunction with the following school Policies/procedures:

- Child Protection Policy and procedures including our Overarching Safeguarding Statement
- CCTV Code of Practice and Procedures
- Data Protection Policy and procedures and related Privacy notices
- Health and Safety Policy and procedures
- Behaviour Policy and procedures
- Whistleblowing Policy and procedures
- Home-School Agreement (part of Welcome Pack)

ONLINE SAFETY GUIDANCE AND 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](#)

Support and resources are also available from:

- [360 Safe - Online safety self-review tool for schools](#)
- [National Centre for Computing Education \(NCCE\)](#)
- [UK Council for Internet Safety](#)
- [UK Safer Internet Centre \(UKSIC\)](#)
- [Education for a Connected World](#)
- [CEOP \(Child Exploitation and Online Protection Centre\)](#)
- [CEOP Education Programme \(Thinkuknow.co.uk\)](#)
- [Cumbria Safeguarding Children Partnership \(Cumbria SCP\)](#)
- [Information Commissioner's Office \(ICO\)](#)
- [Teaching online safety in schools](#)
- [The PREVENT Duty – DfE non-statutory Departmental advice for Schools and Childcare Providers](#)
- [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](#)
- [DotCom Charity](#)
- [Hopes and Streams](#)
- [Internet Matters](#)
- [NSPCC learning](#)
- [Parent Zone's school resources](#)
- [PSHE Association](#)
- [SWGfL](#)

- [Better Internet for Kids](#)
- [Virtual Global Taskforce — 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](#)

APPENDIX A – ONLINE SAFETY – FILTERING AND MONITORING ARRANGEMENTS

1. Introduction

The Department for Education's (DfE) statutory guidance '[Keeping Children Safe in Education](#)' obliges schools in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "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. 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.

'[Keeping Children Safe in Education](#)' 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, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; 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 (e.g. consensual and nonconsensual 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. If we feel our pupils, students or staff are at risk, we will report incidents to the Anti-Phishing Working Group (<https://apwg.org/>).

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/carers 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).

2. DfE Filtering and monitoring standards

The DfE published updated guidance in March 2023 which sets out standards that schools should meet in relation to filtering and monitoring. 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
Identify and assign a member of the Senior Leadership Team to be responsible for ensuring that the standards are met.	Governors - and Online Safety / Safeguarding Link Governor
Identify and assign a Governor to be responsible for ensuring that the standards are met.	
Identify and assign the roles and responsibilities of staff (e.g. school online safety coordinator, Designated Safeguarding Lead) and third parties (e.g. external service providers).	
Document decisions about what is blocked or allowed and why.	
Review the effectiveness of our provision (and	

provide evidence e.g. communication between technical staff and Designated Safeguarding Leads (DSLs).	Head teacher
Oversee reports.	
Ensuring all staff have received appropriate and up to date training, follow Policies, procedures and processes around online safety and filtering and monitoring.	
Ensuring all staff act on reports and concerns.	
Oversee and act on filtering and monitoring reports.	DSL
Oversee and act on safeguarding concerns.	
Oversee and act on checks to monitoring systems.	
Maintain filtering and monitoring systems.	IT Service/Support Provider
Provide filtering and monitoring reports.	
Complete actions following concerns or checks to systems.	
Carry out reviews of the filtering and monitoring provision at least annually.	JOINT (Govs, Head teacher, DSL, and IT Service/Support Provider)
Carry out checks which are informed by the review to ensure systems are working as intended.	

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:

- The Head teacher and a Governor will be responsible for ensuring the standards are met.
- **The roles and responsibilities of individual staff members (e.g. pastoral leads, school online safety coordinator, 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

3. 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 [Keeping Children Safe in Education](#) 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 the Head teacher 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](#))

4. 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 the Head teacher 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 Online Safety Coordinator 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](#).

5. 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	Suggest the user is considering suicide.

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 Head teacher 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/DSL.

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 the Head teacher 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/DDSLs and 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.

Our monitoring system will alert us to behaviours associated with the 4c's as outlined in the section titled [Introduction](#) above.

6. 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 Online Safety Audit](#)
- 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 Head teacher. 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 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 (see below) 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;

- 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.

7. 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.

8. 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](#)

FILTERING AND MONITORING CHECKS - RECORD SHEET

1. System checks - Filtering system

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

2. System checks - Monitoring system

Monitoring System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Monitoring System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Monitoring System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Monitoring System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

LEGAL FRAMEWORK

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should have a copy of The Home Office "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is

important because an offence is complete as soon as the message has been sent; there is no need to prove any intent or purpose.

Data Protection Act 2018 / GDPR

The Data Protection Act 2018 came into force on 25 May 2018. The Act, which replaces the 1998 Act, provides a legal framework for data protection in the UK. It is supplemented by the General Data Protection Regulation (GDPR), the legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).

The General Data Protection Regulation (GDPR) significantly updates previous Data Protection law to reflect changes in technology and the way organisations collect and use information about people in the 21st century. It regulates the processing of personal data and gives rights of privacy protection to all living persons.

Data Controllers are responsible for, and need to be able to demonstrate that they comply with the principles set out in Article 5 of the GDPR which requires that:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data shall be kept for no longer than is necessary.
- Personal data shall be processed in a manner that ensures appropriate security of it.

The first principle of data protection is **fair, lawful and transparent processing**, and is the foundation on which everything else is built.

The Computer Misuse Act 1990 (sections 1 - 3)

This Act makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- “Eavesdrop” on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission. The material to which copyright may attach (known in the business as “work”) must

be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Trademarks Act 1994

This provides protection for Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they must follow a number of set procedures.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts.
- Ascertain compliance with regulatory or self-regulatory practices or procedures.
- Demonstrate standards, which are or ought to be achieved by persons using the system.
- Investigate or detect unauthorised use of the communications system.

- Prevent or detect crime or in the interests of national security.
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Criminal Justice and Immigration Act 2008

- Section 63 – it is an offence to possess “extreme pornographic image”
- Section 63 (6) – the image must be “grossly offensive, disgusting or otherwise obscene”
- Section 63 (7) - this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” and must also be “explicit and realistic”. Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/ Bullying:

- Head teachers have the power, “to such an extent as is reasonable”, to regulate the conduct of pupils off site.
- School staff can confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying procedures.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Human Rights Act 1998

This does not deal with any issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial.
- The right to respect for private and family life, home and correspondence.
- Freedom of thought, conscience and religion.
- Freedom of expression.
- Freedom of assembly.

- Prohibition of discrimination.
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties, and obligations, which arise from other relevant legislation.

ICT ACCEPTABLE USE AGREEMENT – PUPIL/PARENT



Dear Parent,

- Information and Communication Technologies (ICT) including the internet, email, and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
- Please read and discuss these online safety rules with your child and return the slip below to their class teacher. If you have any concerns or would like anything in the agreement explained, then please contact me.
- **Please also take care to ensure that appropriate systems are in place at home to protect and support your child/ren.**

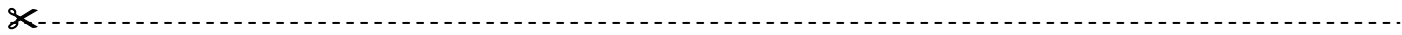
Thank you for your continued support.
Mr. Clem Coady

These rules will help us to be fair to others and keep everyone safe.

- ★ I will only use Information and Communication Technologies (ICT) in school for school purposes.
- ★ I will only use my class email address or my own school email address when emailing.
- ★ I will only open email attachments from people I know, or who my teacher has approved.
- ★ I will not give my username and passwords to anyone else but my parents.
- ★ If I think someone has learned my password, then I will tell my teacher.
- ★ I will only open/delete my own files.
- ★ I will 'log-off' when I leave a computer.
- ★ I will make sure that all ICT contact with other children and adults is responsible, polite, and sensible.
- ★ I will not deliberately look for, save, or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- ★ I will not give out or share my own/or others' details such as name, phone number or home address.
- ★ I will be aware of 'stranger danger' when I am communicating online and will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ★ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ★ I will not capture images, video or voice recordings on my personal device or smart device.
- ★ I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online and I will not show it to other pupils.
- ★ I will support the school approach to online safety and not deliberately upload or

add any images, video, sounds or text that could upset any member of the school community.

- ★ I know that my use of the school ICT systems and email can be checked, and my parent(s) contacted if a member of school staff is concerned about my safety.
- ★ I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.



Stoneraise School

Pupil ICT Acceptable Use – Pupil and Parent Agreement

We have discussed the ICT Acceptable Use Agreement with _____
(child's name) and we will follow the online safety rules and support the safe use of ICT at Stoneraise School.

Parent Name:			
Signed (Parent):		Date:	
Signed (Pupil):		Date:	

ICT ACCEPTABLE USE AGREEMENT – STAFF/VOLUNTEER/GOVERNOR



The use of Information and Communication technologies (ICT - and personal data) such as email, the Internet, and mobile digital devices are an expected part of daily working life in school, and school governance. This ICT Acceptable Use Agreement is designed to ensure that all staff, volunteers and governors are aware of their responsibilities when using any form of data and ICT as it relates to their role in this school.

It applies to any data and ICT used in school, accessed via the school network, the use of school owned devices ICT systems and equipment out of school, and the use of personal equipment/devices in school or in situations related to employment/volunteering/governance at the school.

All staff, volunteers and governors (where they are using data and/or technology in school or in connection with the work of school) are expected to sign this Agreement and always adhere to its content. **Any concerns or clarification should be discussed with the Headteacher, who is also the School's Online Safety Lead.**

This ICT Acceptable Use Agreement is intended to ensure that:

- Staff/Volunteers/Governors are responsible users and stay safe while using technologies for educational, personal, and recreational use;
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- Staff/Volunteers/Governors are protected from potential risk from the use of ICT; and work to ensure that children in their care are safe users.

School networked resources are intended for educational purposes and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or Local Authority, you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or Local Authority into disrepute is not permitted.

All users are required to follow the conditions laid down in this Agreement. Any breach of these conditions may lead to withdrawal of the user's access; monitoring; and/or retrospective investigation of the user's use of the services; and in some instances could lead to criminal prosecution.

- **Staff/Volunteers/Governors will be issued with, and be asked to sign the Acceptable Use Agreement below digitally.**
- **Pupils/Parents will have a modified version of an Acceptable Use Agreement issued to them when they join school (to be found in the Welcome Pack).**

ICT Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

- ★ I understand the ICT requirements found in DfE guidance regarding 'Social contact outside the workplace' / 'Communication with children (including the use of technology)' / 'Use of mobile phones and other mobile technology by staff and other adults in school' / 'Use of technology for remote learning' / and 'Photography, videos and other images'.

Personal Responsibility

- ★ I will be responsible for my behaviour and communications.
- ★ I understand that I am expected to use ICT resources and data for the purposes for which they are made available.
- ★ It is my responsibility to take all reasonable steps to ensure compliance with the conditions set out in this Agreement, and ensure that unacceptable use does not occur.
- ★ I will accept personal responsibility for reporting any misuse of the network or data to the Head teacher.

Keeping Safe

- ★ I understand that all my use of the Internet and other related technologies can be monitored and logged, and made available to the Head teacher/Chair of Governors.
- ★ I will not reveal any personal information (e.g., home address, telephone number, social networking details) of other users to any unauthorised person.
- ★ I will not give out my own personal details, such as mobile phone number, personal email address, personal social media account, or any other social media link, to pupils.
- ★ I will only use my own usernames and passwords which I will choose carefully so they cannot be guessed easily. I will also change the passwords on a regular basis and always where I think someone may have learned my password.
- ★ I will not use any other person's username and password.
- ★ I will not use any other person's username and password or, where they are known, pass the details to any other individual.
- ★ I will not attempt to access other users' files or folders.
- ★ I will ensure that my data is regularly backed up.
- ★ I will ensure that I 'log off' after my network session has finished.
- ★ If I find an unattended computer or other digital device logged on under another user's username, I will **not** continue using the device – I will 'log off' immediately.
- ★ I will ensure that my online activity, both in school and outside school, will not bring my role or the school into disrepute.
- ★ I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
- ★ I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Head teacher as soon as I become aware of the access/receipt.
- ★ I will not accept invitations from pupils to add me as a friend to their social networking sites, nor will I invite them to be friends on mine, unless this has been agreed by the Head teacher or Chair of Governors as acceptable. As damage to professional reputations can inadvertently be caused by quite innocent postings, texts or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my role at the school, such as parents and their children.
- ★ I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:
 - do not reveal confidential information about the way the school operates;
 - are not confused with my school role/responsibilities in any way;
 - do not include inappropriate or defamatory comments about individuals connected with the school community;
 - support the school's approach to online safety which includes not uploading or posting to the Internet any 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.

- ★ I understand that data protection legislation requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school procedures to disclose it to an appropriate authority.
- ★ I will only transport, hold, disclose or share personal information about myself or others as outlined in the school personal data guidelines. I will not send personal information by email as it is not secure.
- ★ Where personal data is transferred outside the secure school network, it must be encrypted. Personal data can only be taken out of school or accessed remotely when authorised, in advance, by the Head teacher or Chair of Governors. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g., on a password secured laptop or memory stick. Staff leading a trip are expected to take relevant pupil information with them, but this must always be held securely.
- ★ I will not attempt to bypass the school network filtering and security systems in place, nor will I use words or phrases to establish if the filtering systems are enabled and working without permission from the Head teacher.
- ★ I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.

Promoting Safe Use by Learners

- ★ I will support and promote the school's Online Safety, Data Protection and Behaviour Policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- ★ I will model safe use of the Internet in school.
- ★ I will educate children on how to use technologies safely according to the school teaching programme.
- ★ I will take immediate action in line with school procedures if an issue arises in school that might compromise a learner, user, or school safety, or if a pupil reports any concerns.

Communication

- ★ I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'acceptable' by the Head teacher or Chair of Governors.
- ★ I will not create, transmit, display, or publish any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person or bring the school or Local Authority into disrepute.
- ★ I will communicate online in a professional manner and tone; I will not use aggressive or inappropriate language and I will appreciate that others may have different opinions.
- ★ I will remember that I am a representative of the school on a global public system.
- ★ I understand that illegal activities of any kind are strictly forbidden. Messages relating to or in support of illegal activities will be reported to the Head teacher or Chair of Governors.
- ★ I am aware that email is not guaranteed to be private.
- ★ I understand that anonymous messages are not permitted.
- ★ I will not engage in any online activity that may compromise my professional responsibilities/role.
- ★ I will not use language that could be calculated to incite hatred against any ethnic, religious, or minority group.
- ★ I will only communicate with pupils and parents using the school's approved, secure email system. Any such communication will be professional in tone and manner.
- ★ I am aware that any communication could be forwarded to the Governing Body or Local Authority, or in some circumstances, the Police.
- ★ I will only use chat and social networking sites that are approved by the school when using school-owned devices.

- ★ I will not use personal email addresses on the school ICT systems unless I have permission to do so.
- ★ I will not send or publish material that violates the Data Protection Act or breaches the security this Act requires for personal data.
- ★ Where work is protected by copyright, I will not download, receive, send, distribute or publish material that violates copyright law. This includes music and videos and materials sent/received using Video Conferencing or Web Broadcasting. If I am unsure about this, I will seek advice from the Head teacher or Chair of Governors.
- ★ I will ensure that any personal data (where the Data Protection Act applies) that is sent over the Internet (or taken off-site in any other way) will be encrypted.

Research and Recreation

- ★ I will not browse, upload, download, distribute or otherwise access any materials which are illegal, discriminatory, or inappropriate or may cause harm or distress to others.
- ★ I will not (unless I have the permission of the Head teacher) make large downloads or uploads that might take up network/internet capacity.
- ★ I know that all school ICT is primarily intended for educational use, and I will only use the systems for personal or recreational use if this is allowed by the school.

Sharing

- ★ I will not access, copy, remove or otherwise alter any other user's file, without their permission.
- ★ I will always respect the privacy and ownership of others' work online and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission, and will credit them if I use it.
- ★ Images of pupils and/or staff will only be taken, stored, and used for professional purposes using school equipment in line with school procedures.
- ★ I will not use my personal equipment (including digital cameras, camera phones, or other digital devices, including use of new technology e.g. smart watch) to create, record or transfer images/video/voice of children or young people unless I have permission to do so from the Head teacher.
- ★ I will only take images/video of pupils and staff where it relates to agreed learning and teaching activities and will ensure I have the Head teacher's and parent's permission before I take them.
- ★ If images are to be published online or in the media, I will ensure that parental/staff permission allows this.
- ★ I will not keep images and/or videos of pupils stored on my personal equipment (and/or in back-up systems for that equipment, including cloud back-ups) unless I have permission from the Head teacher or Chair of Governors to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that for which I have permission.
- ★ Where these images are published (e.g., on the school website/social media), I will ensure that it is not possible to identify the people who are featured by name or other personal information.
- ★ I will not record pupil names in the file names for images/videos.
- ★ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

Buying/Selling/Gaming/Gambling

- ★ I will not use school equipment for online purchasing, selling, gambling or gaming unless I have permission of the Head teacher or Chair of Governors to do so.

General Equipment Use

- ★ I will not use the network in any way that would disrupt the use of the network by others.
- ★ I will not use 'USB drives', portable hard-drives, tablets or personal laptops on the network without having them 'approved' by the Head teacher and checked for viruses.
- ★ I will not download or install any hardware or software on a computer or other device without the permission of the Head teacher. Nor will I download or install any unapproved software, system utilities or resources from the Internet that might compromise the network or not be adequately licensed.
- ★ I will not try to alter computer settings without the permission of the Head teacher.
- ★ I will not cause damage to ICT equipment in school, or attempt to harm or destroy any equipment or data of another user or network connected to the school system.
- ★ I will immediately report any illegal, inappropriate, or harmful material or incident I become aware of, to the Head teacher.
- ★ I will immediately report any damage or faults involving equipment or software; however this may have happened.
- ★ I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- ★ I will inform the Head teacher immediately if a security problem is identified and will not demonstrate this problem to other users.
- ★ I understand that I must comply with the ICT Acceptable Use Agreement of any other network which is accessed via the school network.
- ★ I understand that files held on the school's network will be regularly checked and monitored, and that users identified as a security risk will be denied access to the network.
- ★ I understand this ICT Acceptable Use Agreement forms part of the terms and conditions set out in my contract of employment.
- ★ I understand that if I fail to comply with this ICT Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

Stoneraise School – ICT Acceptable Use Agreement – Staff/Volunteer/Governor

I have read, understood and agree to follow the school rules regarding ICT, data, and use of the school network as described in the:

- ICT Acceptable Use Agreement – Staff/Volunteers/Governors;
- Online Safety Policy & procedures; and
- DfE guidance relating to Online Safety and Teacher Standards

I will use the school network and school-owned devices in a responsible way and observe all the restrictions as explained in the staff/volunteer/governor ICT Acceptable Use Agreement. If I am in any doubt, I will consult the Head teacher. I agree to use ICT and data by these rules when:

- ✓ I use school ICT systems and/or equipment and school-owned devices at school, at home, or in other public or private spaces when I have permission to.
- ✓ I use my own ICT (where permitted) in school and will adhere to the ICT Acceptable Use Agreement in relation to the use of my own personal devices/technology.
- ✓ I use my own ICT out of school to access school sites or for activities relating to my employment, volunteering, or governance for school.

If I do not follow the rules, I understand that this may result in loss of access to these resources and/or disciplinary action. I also understand that persons under reasonable suspicion of misuse in terms of access or content may be placed under retrospective investigation or have their usage monitored.

A Google Form will be sent out for staff/volunteers/governors to respond to each time the Online Safety Policy is reviewed.