Wykeham Primary

Committed to Excellence, Equality and Enjoyment

Wykeham Primary School

Online Safety Policy

Updated: January 2019

Presented and Agreed by Governors: February 2019

Signed by Co Chair of Governors:

Signed by Headteacher:

Review Date: January 2021

Wykeham Primary School
Online Safety Policy

Wykeham Primary School is committed to safeguarding and promoting the welfare of children as we believe that this is of paramount importance. We expect all staff and volunteers to share this commitment.

We uphold the rights of everyone to equality under the law regardless of gender, age, race, belief, ability, disability, sexual orientation or identity.

We believe that our core school values of respect, responsibility, tolerance and co-operation and the British values are not mutually exclusive. We focus on ensuring our work is effective in securing these values; challenging children, staff and parents who express opinions contrary to the British values with regard to our duty to prevent extremism and radicalisation.

Wykeham School has the highest regard for the safety of the children in our care. Every adult who works at the school has been trained to appreciate that they have a key responsibility for keeping children safe at all times.

This policy applies to all members of Wykeham Primary School community, including staff, pupils, volunteers, parents/carers, visitors, community users, who have access to and are users of the school information technology systems, both in and out of Wykeham Primary School.

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

1 Introduction

At Wykeham Primary School the health, safety and well-being of all our staff and pupils are of paramount importance to all the adults who work in our school. Our pupils have the right to protection from all types of harm or abuse. It is our duty to ensure that every pupil in our care is safe, and that the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

The Education and Inspections Act 2006 empowers headteachers 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 is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. Further, in line with the DfE guidance 'Searching, screening and confiscation: advice for schools' (2018) – Section 15,

the Headteacher and staff authorised by him have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying. In the case of both acts, action can only be taken over issues covered by the school's Behaviour and Discipline Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

2 Aims and Objectives

This policy aims to:

- Set out the high expectations for all Wykeham Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline);
- Ensure all stakeholders recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform;
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning through all school activities, both within the curriculum and outside the classroom.
- Increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online;
- Ensure school staff working with children understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice;
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession;
- Follow clear structures and procedures for any inappropriate online behaviour and where there are doubts or concerns (please refer to other school policies - Behaviour and Discipline Policy and Anti-Bullying Policy).

3 The Main Areas of Risk for Pupils in our School Community

3.1 Content

- exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- lifestyle websites, for example videos showing how to make harmful materials, pro-anorexia/self-harm/suicide sites;
- hate sites;
- grooming;
- radicalisation;
- content validation: how to check authenticity and accuracy of online content.

3.2 Contact

- grooming;
- cyber-bullying in all forms;
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords.

3.3 Conduct

- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (internet or gaming));
- sexting (sending and receiving of personally intimate images) also referred to as self-generated indecent images (SGII);
- copyright (little care or consideration for intellectual property and ownership – such as music and film) (ref Ofsted 2013).

4 Education and Curriculum

4.1 Pupil Online Safety Curriculum

The following subjects have the clearest online safety links:

- Computing
- Personal, Social, Health, Citizenship and Economics Education (PSHCE)

However, it is the role of all staff to identify opportunities to secure the importance of thread online safety through all school activities, and making the most of unexpected learning opportunities as they arise, which have a unique value for pupils.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as home learning tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites, despite appropriate filtering and monitoring in place at school.

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 and data law.

At Wykeham Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and as such, we have adopted the cross-curricular framework 'Education for a Connected World' from United Kingdom Council for Child Internet Safety (UKCCIS).

Annual reviews of curriculum plans (including for pupils with special educational needs and disabilities (SEND) are used as an opportunity to follow this framework more closely in its key areas of:

- Self-image and Identity,
- Online relationships,
- Online reputation,
- Online bullying,
- Managing online information,
- Health, wellbeing and lifestyle,
- Privacy and security, and
- Copyright and ownership.

4.2 Staff and Governor Training

Our school ensures staff and governors know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

Our school makes annual training available to governors and staff on online safety issues and the school's online safety education program, with updates at weekly staff meetings as necessary;

Our school provides as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

4.3 Parent Awareness and Training

Our school runs a rolling programme of advice, guidance and training for parents, including:

- introduction of the Acceptable Use Agreements to all parents, to ensure that principles of online safety behaviour are made clear
- information leaflets; in school newsletters; on the school website;
- demonstrations, practical sessions held at school;

- suggestions for safe Internet use at home; and
- provision of information about national support sites for parents.

5. Expected Conduct

5.1 In our school, all users:

- are responsible for using the school information and communication systems in accordance with the relevant Acceptable Use Agreements, which they will be expected to sign before being given access to school systems (at EYFS, it is expected that parents/carers would sign on behalf of the pupils);
- need to understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school;
- know and understand school policies on the use of mobile and hand held devices, including cameras. They should also know and understand school policies on the taking/use of images and on online bullying.

5.2 Staff are responsible for reading the school's Online Safety Policy and using the school ICT systems accordingly, including the use of mobile phones and hand held devices.

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

5.4 Parents/carers should provide consent for pupils to use the internet, as well as other technologies, as part of the online safety Acceptable Use Agreement form. Parents/carers should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

6 Handling Online Safety Concerns

6.1 It is vital that all staff recognise that online safety is a part of safeguarding, as well as being a curriculum strand of Computing, PSHCE, Citizenship and (from September 2019 for September 2020) the new statutory Health Education and Relationships Education.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the Online Safety Lead / Designated Safeguarding Lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching 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).

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

- Safeguarding and Child Protection Policy
- Peer on Peer Abuse Policy
- Anti-Bullying Policy
- Behaviour and Discipline Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation.

The school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly in order for the issues to be dealt with quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the Online Safety Lead (OSL) or the Designated Safeguarding Lead (DSL)on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher, in which case, the compliant is referred to the Chair of Governors. Staff may also use guidelines provided in the Whistleblowing Policy.

The school will actively seek support from other agencies as needed. We will inform parents/carers of online safety incidents involving their children, and the Police, where staff or pupils engage in or are subject to behavior, which the school considers to be particularly disturbing, or behaviour that break the law.

6.2 Sexting

Our school uses the UKCCIS guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. We recognize that in many instances, it might be someone other than the DSL or OSL to first become aware of an incident, and it is vital that the correct steps be taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school's DSL will in turn use the guidance provided to decide next steps and whether other agencies need to be involved. It is important that everyone understands that whilst sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

6.3 Bullying

Online bullying should be treated like any other form of bullying and the school's Anti-bullying Policy should be followed for online bullying, which may also be referred to as cyberbullying.

6.4 Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) must be reported to the DSL who will follow the full guidance as outlined within Keeping Children Safe in Education (2018). Staff work to foster a zero-tolerance culture. Wykeham Primary School takes all forms of sexual violence and harassment seriously and staff take appropriate action in accordance with the Child Protection Policy. If in any doubt, staff should speak to the DSL (or deputy DSL). This discussion should be handled sensitively and with the support of children's social care if required. In cases where the alleged sexual violence or sexual harassment involves pupils from the same school, but is alleged to have taken place away from the school premises, or online, the safeguarding principles, and the school's duties to safeguard and promote the welfare of pupils remain the same.

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

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Acceptable Use Policy as well as in other school policies. Where pupils contravene these rules, the school's Behaviour and Discipline Policy will be applied; where staff contravenes these rules, action will be taken as outlined in the staff Code of Conduct Policy. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

6.6 Social media incidents

All users are expected to follow the rules of appropriate behaviour at Wykeham Primary School. These are also governed by the school's Acceptable Use Policies and other related policies. Breaches will be dealt with in line with the school Behaviour and Discipline Policy (for pupils) or Code of Conduct Policy (for staff). Further to this, where an

incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

6.7 Data Protection and Data Security

The Headteacher, Data Protection Officer (DPO) and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that safeguarding is always put first and data-protection processes support careful and legal sharing of information. Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

7. Actions where there is a concern about a child

While the school takes all reasonable precautions to ensure online safety, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

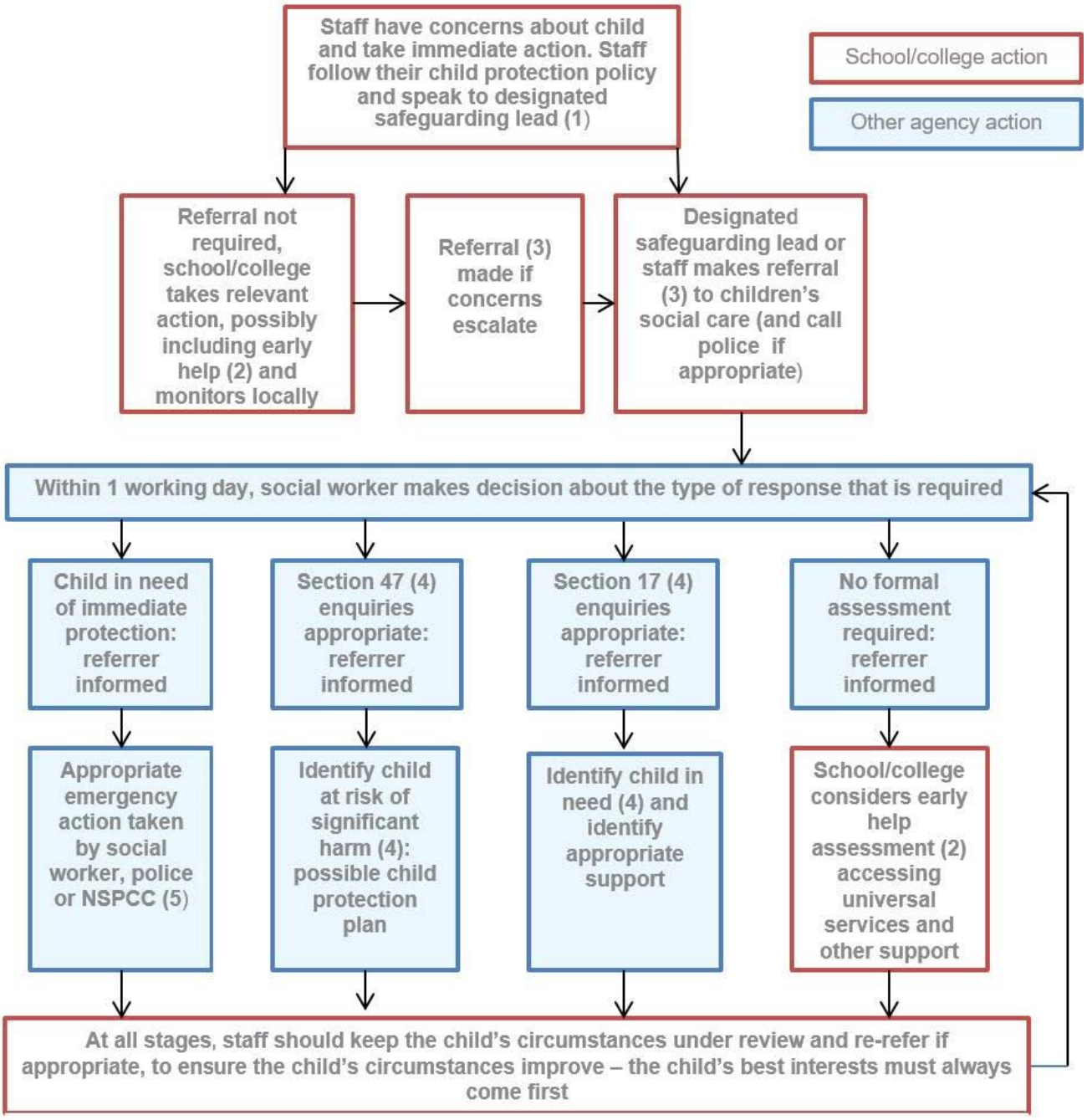
Staff and pupils are given information about infringements in use and possible sanctions. Sanctions used include:

- discussion with the class teacher with follow-up discussion with Online Safety Coordinator/ Headteacher as necessary;
- informing parents or carers;
- removal of internet or computer access for a period of time (which could ultimately prevent access to files held on the system, including homework);
- referral to Local Authority or Police.

Our Online Safety Coordinator acts as our first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with our Child Protection and Safeguarding Policy.

As outlined below, online safety concerns are no different to any other safeguarding concern. The following chart outlines our procedure:



(1) In cases which also involve an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working together to safeguard children provides detailed guidance on the early help process.

(3) Referrals should follow the local authority's referral process. Chapter one of Working together to safeguard children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. This can include section 17 assessments of children in need and section 47 assessments of children at risk of significant harm. Full details are in Chapter One of Working together to safeguard children.

(5) This could include applying for an Emergency Protection Order (EPO).

8 Communication

This policy will be communicated to staff/pupils/community in the following ways:

- it is posted on the school's website and on the school's intranet;
- it is a part of school induction pack for new staff;
- Pupils'/Staff's Acceptable Use Agreements are discussed with and signed by pupils/staff at the start of each year;
- Parents sign Acceptable Use Agreements at the start of each year;
- signed Acceptable Use Agreements are displayed in classrooms.

9. Monitoring and Review

The Online Safety Policy is referenced from within other school policies: Computing Policy, Child Protection and Safeguarding Policy, Anti-Bullying Policy and in the School Development Plan, Behaviour and Discipline Policy, Personal, Social and Health and Citizenship Education Policies.

The school has an Online Safety Coordinator who will be responsible for document ownership, review and updates.

The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

The Online Safety Policy has been written by the school's Online Safety Coordinator and is current and appropriate for its intended audience and purpose.

There is widespread ownership of the policy and it has been agreed to by the Core Leadership Team and approved by governors and other stakeholders. All amendments to the school Online Safety Policy will be discussed with all members of teaching staff.

Appendix 1: Roles and Responsibilities

Key Responsibilities for Headteacher:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding;
- Oversee the activities of the Designated Safeguarding Lead/Online Safety Lead, and ensure that their responsibilities listed in the sections below are being followed and fully supported;
- Ensure that policies and procedures are followed by all staff;
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance;
- Liaise with the Designated Safeguarding Lead/Online Safety Lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information;
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that safeguarding is always put first and data-protection processes support careful and legal sharing of information;
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles;
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles;
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident;
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised;
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online safety procedures;
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety;
- Ensure the school website meets statutory DfE requirements.

Key Responsibilities for Designated Safeguarding Lead (DSL):

- The DSL should take lead responsibility for safeguarding and child protection (including online safety).
- The DSL or deputy DSL maintains regular review and open communication with the online safety lead.
- Liaise with the Local Authority and work with other agencies in line with 'Working together to safeguard children'.
- Work with the Headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child

protection is always put first and data-protection processes support careful and legal sharing of information.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- Facilitate training and advice for all staff:
  - all staff must read KCSIE (2018) Part 1 and all those working with children Annex A.

Key Responsibilities for Online Safety Lead:

- Ensure an effective approach to online safety that empowers the school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Stays up to date with the latest trends in online safety.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCCIS framework 'Education for a Connected World') and beyond, in wider school life.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents.
- Communicate regularly with the Core Leadership Team (CLT) and the designated online safety governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how the school's filtering and monitoring procedures work.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based, in harmony with policies for behaviour, safeguarding, Prevent and others.
- Oversee and discuss 'appropriate filtering and monitoring' with staff and ensure they are aware of the filtering service provided by LGfL.
- Facilitate training and advice for all staff:
  - all staff should be familiar with KCSIE (2018) Annex C (online safety).
  - cascade knowledge of risks and opportunities throughout the organisation.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Key Responsibilities for Governing Body, led by Online Safety/ Safeguarding Link Governor:

- Approve this policy and strategy and subsequently review its effectiveness.
- Ensure an appropriate senior member of staff, from the school's leadership team, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety).
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Ensure that there is regular review and open communication between the DSL and online safety coordinator and that the DSL's clear overarching responsibility for online safety is not compromised.
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE (2018); CLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in the school.
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and regularly updated in line with advice from the LSCB. Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.
- Ensure appropriate filters and appropriate monitoring systems are in place, being aware that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology.

Key Responsibilities for All staff:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for CLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.

- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the staff Acceptable Use Policy and Code of Conduct Policy.
- Notify the DSL/OSL if this 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 subject leaders, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Encourage pupils to follow their Acceptable Use Policy, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Be aware that you are often most likely to see or overhear online safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know.
- Receive regular updates from the DSL/OSL 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 of the professional reputation of all staff.

Key Responsibilities for PSHCE Lead and Relationships Educations Lead:

Key responsibilities from September 2019 for September 2020:

- As listed in the ‘all staff’ section, plus:
- Embed mental wellbeing, healthy relationships and staying safe online into the PSHCE/Relationships Education curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHCE / RE.

Key Responsibilities for Computing Curriculum Lead:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable use agreements.

Key Responsibilities for Subject Leaders:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCCIS framework Education for a Connected World can be applied in your context.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

Key Responsibilities for Network Manager/Technician:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the Designated Safeguarding Lead/Online Safety Lead /Data Protection Officer to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (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.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and Core Leadership Team.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.

- Utilise the services provided by LGfL and take advantage of the following solutions which are part of the package bought into by the school: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare. These solutions aim to help protect the network and users on it.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.

Key Responsibilities for Data Protection Officer (DPO):

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' (2018) and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
  - GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. 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 should still be in place. Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding.
- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'.
- Work with the DSL, Headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Key Responsibilities for Volunteers and Contractors:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP).
- Report any concerns, no matter how small, to the Designated Safety Lead / Online Safety Lead as named in the AUP.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

Key Responsibilities for Pupils:

- Read, understand, sign and adhere to the pupil acceptable use policy and review this annually.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Key Responsibilities for Parents/Carers:

- Read, sign and promote the school's parental Acceptable Use Policy (AUP) and read the pupil AUP and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Key Responsibilities for External groups/individuals:

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

Appendisx 2: Acceptable Use Policy (AUP) for Staff, Governros and Volunteers

This agreement covers use of all digital technologies while in school, that is, **email, internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, apps **and other relevant digital systems provided by the school or school umbrella body (London Grid for Learning).**

It also covers school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

Wykeham Primary School regularly reviews and updates all Acceptable Use Policy (AUP) documents to ensure that they are consistent with our school's Online Safety Policy. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

Agreement:

1. I have read and understood Wykeham Primary School's full Online Safety Policy [www.wykeham.brent.sch.uk/our-school/policies] and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Leads (Denise Springer/Gurvinder Notay) or Headteacher (Everton Sharpe).
3. I understand the responsibilities listed for my role in the school's Online Safety Policy and agree to abide by these.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in our school's Online Safety Policy. I will report any breach of this by others.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices are stated in these respective policies. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, that of the school and of the teaching profession, and I will do nothing to impair either.
9. I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.
10. I agree to adhere to all provisions of our school's Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share

credentials and immediately change passwords and notify the Headteacher if I suspect a breach. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

11. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring, will look after devices loaned to me, and will notify the school of "significant personal use" as defined by HM Revenue & Customs.
12. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
13. I understand and support the commitments made by pupils/students, parents/carers, fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
14. I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might think are unimportant – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture, but only if I tell somebody. I have read the sections on handling incidents and concerns about a child in general, sexting, bullying, sexual violence and harassment, misuse of technology and social media.
15. I understand that breach of this AUP and/or of our school's Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent Online Safety Policy and Safeguarding Policy. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by the Headteacher/Deputy Headteacher/Online Safety Coordinator

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: _____

Name: _____

Role: _____

Date: _____

Appendix 3: Acceptable Use Policy (AUP) for KS1 Pupils

This is how we keep **SAFE online**:	✓
1. We only use the devices we're **ALLOWED** to.	
2. We **CHECK** before we use new sites, games or apps.	
3. We **ASK** for help if we're stuck.	
4. We **KNOW** people online aren't always who they say.	
5. We don't keep **SECRETS** just because someone asks us to.	
6. We don't change **CLOTHES** in front of a camera.	
7. We are **RESPONSIBLE** and never share private information.	
8. We are **KIND** and polite to everyone.	
9. We **TELL** a trusted adult if we're worried, scared or just not sure.	
10. If we get a **FUNNY FEELING** in our tummy, we talk to an adult.	

Our trusted adults are _____ at school,

_____ at home and _____

Appendix 4: **Acceptable Use Policy (AUP) for KS2 Pupils**

This agreement will help keep us safe and help us to be fair to others

1. ***I learn online*** – I use the school's internet and devices for school activities, home learning and other activities to learn and have fun. I only use apps, sites and games if a trusted adult says I can.
2. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people; I get creative to learn and make things!
3. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. If I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
4. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
5. ***I am careful what I click on*** – I don't click on links I don't expect to see and only download or install things when I know it is safe or has been agreed by trusted adults.
6. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game as it often helps. If I get a funny feeling, I talk about it.
7. ***I know it's not my fault if I see or someone sends me something bad*** – I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell my parent/carer, teacher or other trusted adult.
8. ***I communicate and collaborate online*** – I will only communicate with people I know and have met in real life or that a trusted adult knows about.
9. ***I know new friends aren't always who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. If I want to meet them, I will ask my parent/carer, and never go alone or without telling an adult.
10. ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and with whom.
11. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
12. ***I am private online*** – I only give out private information if my parent/carer says it's okay. This might be my home address, phone

number or other personal information that could be used to identify me or my family and friends.

13. ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only. I don't send any photos without checking with a trusted adult.
14. ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
15. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour.
16. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see any of these.
17. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
18. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
19. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

Our trusted adults are _____ at school and

_____ at home.

We have read this agreement. We know who our trusted adults are and agree to the above.

Appendix 5: Acceptable Use Policy (AUP) for Parents

What is an AUP?

We ask all children, young people and adults involved in the life of Wykeham Primary School to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
Your child has also signed an AUP which is available from your child's class teacher should you wish to see it.

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.
School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.
We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read Wykeham's full Online Safety Policy [www.wykeham.brent.sch.uk] for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to Mrs Brazer or your child's teacher.

What am I agreeing to?

1. I understand that Wykeham Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety. Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. (Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK).
9. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which is available upon my request, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
10. I can find out more about online safety at Wykeham Primary School by reading the full Online Safety Policy here (www.wykeham.brent.sch.uk) and can talk to my child's teacher if I have any concerns about my child's/children's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____