



Online Safety Policy

This policy applies all pupils in the school, including in the EYFS

Signed:	<u>S. Ruddock</u>
Chair of Local Advisory Board:	Sharma Ruddock
Approved:	September 2020
Review Period	2 years
Review Date:	September 2022

Introduction

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ September 2021 (KCSIE) and other statutory documents; it is designed to sit alongside your school’s statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school’s safeguarding and child protection procedures. KCSIE makes clear that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).”

Contents

Contents.....	2
Overview	4
Aims.....	4
Further Help and Support	4
Scope	4
Roles and responsibilities	5
Headteacher – Sally Quartson	5
Designated Safeguarding Lead – Eve Watson.....	6
Local Advisory Board, led by Online Safety/Safeguarding Link Member	7
All Staff	8
PSHCEE / Relationships Education Lead – Jayne Aherne.....	9
Computing Curriculum Lead – Ashleigh van Bergen.....	9
Network Manager/Technician – Elizabeth Renouf Crotty / Dataspire	9
Data Protection Officer (DPO) – Stuart Dixon (BPET)	10
Volunteers and Contractors	10
Pupils	11
Parents/Carers	11
External Groups including Parent Associations	11
Education and Curriculum	12
Handling Online-Safety Concerns and Incidents	12
Actions - Where there are concerns about a child	14
Sexting.....	15
Bullying.....	15
Sexual Violence and Harassment.....	15
Misuse of School Technology (Devices, Systems, Networks or Platforms)	16
Social Media Incidents	16
Data Protection and Data Security	17
Appropriate Filtering and Monitoring	17
Electronic Communications	18
Email.....	18
Zoom	19
Class Dojo	20
School Website	20
Cloud Platforms	20

Digital Images and Video	20
Social Media	21
Watling Park’s SM Presence.....	22
Staff, Pupils’ and Parents’ SM Presence	22
Device Usage.....	23
Personal Devices and Bring Your Own Device (BYOD) Policy	23
Network / Internet Access on Personal Devices	24
Trips / Events Away from School	24
Searching and Confiscation	24

Overview

Aims

This policy aims to:

- Set out expectations for all Watling Park community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care;
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice;
 - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and the headteacher will handle referrals to the LA designated officer (LADO). The local authority, trust or third-party support organisations may also have advisors to offer general support.

Beyond this, [reporting.lgfl.net](https://www.lgfl.net/reporting) has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre, the NSPCC Whistleblowing Helpline, hotlines for hate crime, terrorism and fraud, and anonymous support for children and young people.

Scope

This policy applies to all members of the Watling Park community (including staff, Local Advisory Board members, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher – Sally Quartson

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section 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 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 Local Advisory Board to ensure a GDPR-compliant framework for storing data which helps to ensure that child protection 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 the needs of the 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 the Local Advisory Board are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory DfE requirements.

Designated Safeguarding Lead – Georgina Harcourt-Brown

Key responsibilities (the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2021):

- “The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).”
- Ensure “An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
- “Liaise with the local authority and work with other agencies in line with Working together to safeguard children.”
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the headteacher, DPO and Local Advisory Board to ensure a GDPR-compliant framework for storing data helps to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safety – the LGfL DigiSafe [pupil survey](#) of 40,000 pupils may be useful reading (new themes include ‘self-harm bullying’ and getting undressed on camera).
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the Local Advisory Board/trustees.
- 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 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.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Communicate regularly with SLT and the designated online safety Local Advisory Board member to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring.
- 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.
- Oversee and discuss ‘appropriate filtering and monitoring’ with the Local Advisory Board (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this).
- 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 Part 1 and all those working with children Annex A;

- it would also be advisable for all staff to be aware of Annex C (online safety);
- cascade knowledge of risks and opportunities throughout the organisation.

Local Advisory Board, led by Online Safety/Safeguarding Link Member

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2018 – updated 2021):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCCIS) [Online safety in schools and colleges: Questions from the Governing Board](#).
- “Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support...”
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at Local Advisory Board meetings.
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data helps 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; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your 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 [but...] be careful 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:

- 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) is.
- 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 SLT 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/handbook.
- Notify the DSL if policy does not reflect practice in your 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 (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 homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).
- 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/students to follow their acceptable use policy, remind them about it and enforce school sanctions.
- 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.
- 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 know.
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe [pupil survey](#) of 40,000 pupils (new themes include 'self-harm bullying' and getting undressed on camera).
- 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.

PSHCE / Relationships Education Lead – Jayne Aherne

- As listed in the ‘all staff’ section.
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHCEE/ 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 and all other staff to ensure an understanding of the issues, approaches and messaging within PSHCEE/Relationships Education.

Computing Curriculum Lead – Luke Morgan

Key responsibilities:

- As listed in the ‘all staff’ section.
- 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.

Network Manager/Technician – Elizabeth Renouf Crotty / Dataspire

Key responsibilities:

- As listed in the ‘all staff’ section.
- 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/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 senior 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.

- 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.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – Mark Greatrex (BPET)

Key responsibilities:

- NB – this document is not for general data-protection guidance.
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ 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
- Work with the DSL, headteacher and Local Advisory Board to ensure frameworks are in place for the protection of data and of safeguarding information sharing.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and Contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy.
- 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.
- 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.

Parents/Carers

Key responsibilities:

- 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, Local Advisory Board members, contractors, pupils or other parents/carers.
- Respect age ratings on social media and gaming platforms wherever possible and not encourage or condone underage use.

External Groups including Parent Associations

Key responsibilities:

- 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, Local Advisory Board members, contractors, pupils or other parents/carers.

Education and Curriculum

At Watling Park, we recognise that online safety and broader digital resilience must be thread throughout the curriculum. The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHCEE
- Relationships Education (being implemented from September 2019 for September 2020)
- Computing

However, as stated in the role descriptors above, 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 curriculum/stage/subject leads, 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 homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

Handling Online-Safety Concerns and Incidents

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 and the new statutory 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 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 (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies – Staff, Pupils and Parents
- Prevent Policy

- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc.)
- Staff Code of Conduct/Handbook

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

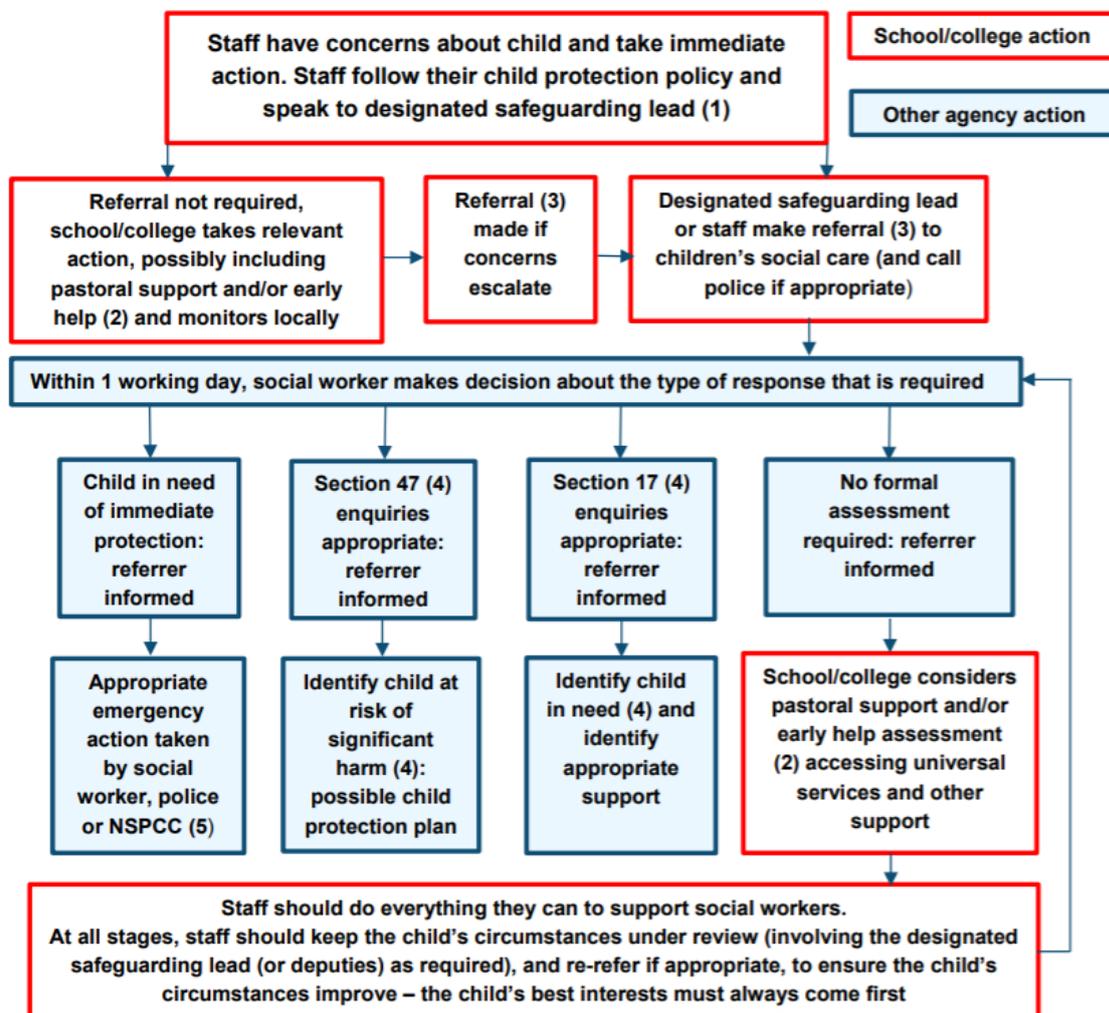
Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Local Advisory Board and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). 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 behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting; see section below).

Actions - Where there are concerns about a child

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2018 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



(1) In cases which also involve a concern or 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 process set out in the local threshold document and local protocol for assessment. 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. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of [Working Together to Safeguard Children](#).

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

Sexting

All schools (regardless of phase) should refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as ‘youth produced sexual imagery’) in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) who first becomes aware of an incident, and it is vital that the correct steps are 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 DSL will in turn use the full 50-page guidance document including case studies, typologies and flow chart to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Bullying

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

Materials to support teaching about bullying and useful Department for Education guidance and case studies can be found at bullying.lgfl.net

Sexual Violence and Harassment

In 2018 new Department for Education guidance was issued on sexual violence and harassment, as a new section within Keeping Children Safe in Education and also a document in its own right.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as ‘low level’ are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

The following is an excerpt from section 46 on page 21 of that document:

“As with all safeguarding concerns, it is important that in such instances staff take appropriate action in accordance with their child protection policy. They should not assume that someone else is responding to any incident or concern. If in any doubt, they should speak to the designated safeguarding lead (or a

deputy). In such cases, the basic safeguarding principles remain the same, but it is important for the school or college to understand why the victim has chosen not to make a report themselves. This discussion should be handled sensitively and with the support of children's social care if required. There may be reports where the alleged sexual violence or sexual harassment involves pupils or students from the same school or college, but is alleged to have taken place away from the school or college premises, or online. There may also be reports where the children concerned attend two or more different schools or colleges. The safeguarding principles, and individual schools' and colleges' duties to safeguard and promote the welfare of their pupils and students, remain the same. The same principles and processes as set out from paragraph 48 will apply. In such circumstances, appropriate information sharing and effective multi-agency working will be especially important."

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 this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

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.

Social Media Incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Watling Park community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (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, Watling Park 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.

Data Protection and Data Security

This section serves to highlight general principles regarding the relationship between safeguarding and data protection/data security, and to signpost to useful information.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

“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.”**

All pupils, staff, Local Advisory Board members, volunteers, contractors and parents are bound by the school’s data protection policy and agreements.

The headteacher, DPO and Local Advisory Board work together to ensure a GDPR-compliant framework for storing data which helps to ensure that child protection 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.

Appropriate Filtering and Monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] 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.”

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Electronic Communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Pupils at this school use the Purple Mash system for all school emails
- Staff at this school use Microsoft Office 365 for all school emails

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and pupils/staff and parents (in both directions). Use of a different platform must be approved in advance by the data protection officer/headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email. If data needs to be shared with external agencies, encryption should be utilised.
- Pupils are restricted to emailing within the school and cannot email external accounts.
- 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.
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but 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.
- Pupils are NOT allowed to use the 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.

See also the social media section of this policy.

Zoom

When using Zoom as an online tool to enhance communication and teaching and learning, all members of the Watling Park School Community must follow the expectations laid out in this document. Additionally, staff must follow these guidelines to ensure the safety of all participants.

- All participant must give express consent to attend and have Zoom calls recorded before being admitted into the call.
- Group sizes must have a minimum of 2 pupil participants and must not exceed 15 pupils. Staff should not engage in 1:1 Zoom calls without the express permission of the Head Teacher.
- Zoom meeting invitations are to be shared directly with participants and not in a group forum.
- Staff must host the Zoom call on a device that allows them to see all participants at once (Laptop or desktop computer).
- Before admitting any children to the Zoom Meeting, staff should begin recording. After the meeting is finished, recordings should be saved on the school server.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background. If needed, staff may hold meetings from school in designated rooms.
- Language must be professional and appropriate, including any family members in the background.
- Videos may be muted for both pupils and staff if other children in the household become unsettled or cause a disruption.

As the meeting host, every staff member has a variety of controls they can use to secure their meeting. By default, Zoom has enabled the Waiting Room feature, required a meeting password, and set screen sharing to "Host Only" for a more secure meeting. For more information, visit <https://support.zoom.us/hc/en-us/articles/115005759423>

- Prevent Participants from Screen Sharing: By default, only hosts are able to screen share to prevent disruptions. If you choose to allow others to share, the host can click the arrow next to Share Screen and click Advanced Sharing Options. Under "Who can share?" choose "All Participants" and close the window.
- Waiting Room: By default, waiting room has been enabled which allows the host to control when a participant joins a meeting. When in a meeting, click manage participants and "Admit" to allow participants into your meeting.
- Meeting Password: By default, Zoom requires a meeting password for education. When creating a meeting, the password is embedded into the meeting/webinar links. When manually entering a meeting ID, the user will always be prompted to enter the password.
- Lock the Meeting: when you're in the meeting, click Participants at the bottom of your Zoom window. In the participants pop-up box, you will see a button that says Lock Meeting. When you lock the meeting, no new participants can join, even if they have the meeting ID and password.
- Expel a Participant: still in that participants menu, you can mouse over a participant's name, and several options will appear, including Remove. Click that to kick a participant out of the meeting. They can't get back in if you then click Lock Meeting.

- Attendee On-Hold: if you need a private moment, you can put attendees on-hold. The attendee's video and audio connections will be disabled momentarily. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate this feature.
- Disabling Video: Instructors can turn participant video off and request to start participant video. This will allow instructors to block unwanted, distracting or inappropriate gestures on video.
- Mute participants or Mute All: Instructors can turn mute / unmute participants or all. This will allow instructors to block unwanted, distracting or inappropriate noise from the meeting.

Class Dojo

Class Dojo has been selected as the primary tool of electronic communication between staff and parents at Watling Park School. It can be used to update whole classes and message individual parents.

Staff must follow the pupil-staff communications expectation in the overall school Safeguarding Policy, and must act in accordance with the Data Protection Policy.

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 Headteacher has delegated the day-to-day responsibility of updating the content of the website to Ashleigh Van Bergen and Elizabeth Renouf Crotty.

The Department for Education has determined information which must be available on a school website.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember not to save images with a filename that includes a pupil's full name).

Cloud Platforms

Like many schools we recognise the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning. As a school we utilise Microsoft Office 365/OneDrive.

This school adheres to the principles of the Department for Education document '[Cloud computing services: guidance for school leaders, school staff and governing bodies](#)'.

Digital Images and Video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent).

- For displays around the school

- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than their first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Watling Park, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social Media

Watling Park's SM Presence

Watling Park works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

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

Staff, Pupils' and Parents' SM Presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints 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 (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night/in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, Local Advisory Board members, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, Local Advisory Board members, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, 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 Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 19) and permission is sought before uploading photographs, videos or any other information about other people.

Device Usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal Devices and Bring Your Own Device (BYOD) Policy

- **Pupils** within Years 5 and 6 (who are independent travellers) are allowed to bring mobile phones in to school for emergency use. During the school day, mobile phones should be switched off and looked after by class teachers. Any important messages and phone calls to or from parents can be made through the school office.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded

onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

- **Volunteers, contractors, and members of the Local Advisory Board** should turn their phones to silent and keep them out of sight. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to turn their phones to silent and keep them out of sight whilst on the school premises, including during drop off and collection. Reminder posters are displayed at all entrances to the grounds. Permission should be sought, including whilst attending trips and events, before taking any photos, e.g. of displays in corridors or classrooms, and should avoid capturing other children.

Network / Internet Access on Personal Devices

- **Pupils/students** are not allowed networked access via personal devices.
- **All staff who work directly with children** can access the wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Volunteers, contractors, and members of the Local Advisory Board** can access the wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / Events Away from School

For school trips/events away from school, teachers will be issued with a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing their private phone number.

Searching and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them 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.

Full details of the school's search procedures are available in the school Behaviour Policy.