Online Safety Guidance Policy

This policy is applicable to: All schools in the Wonder Learning Partnership (WLP)

Version 1.0

Important: This document can only be considered valid when viewed on the Website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.	
Name of Responsible Committee/Individual:	LGB & Board of Trustees
Implementation Date:	September 2024
Review Date:	September 2025
Target Audience:	Trust employees, agency workers, self-employed worker and professional visitors including contractors
Reference Documents:	Keeping Children Safe in Education 2023 Regulated Activity in relation to children: scope Working Together to Safeguard Children 2018 Section 175 of the Education Act 2002
Related Documents	Behaviour Policy Anti-Bullying Special Educational Needs Health and Safety Safe Working Practice Guidance Whistleblowing Policy Mental Health Policy and Strategy (DRAFT) Sex & Relationships Education ICT Code of Conduct Off-site learning: arrangements and procedures

Online Safety Policy 2024

(to be reviewed Autumn 2024 in accordance with LA guidance and in line with *Keeping Children Safe in Education September 2024 or sooner if policy changes demand*)

For the purpose of this Policy:

- **'Staff'** refers to all paid adults, volunteers or pupils and students on placement, working in any capacity in the school or in activities organised by the school, which brings them into contact with the pupils/pupils and students of the school.
- **'Parent/s'** refers to adults with parental responsibility for a particular child.
- **DSL –** Designated Safeguarding Lead
- **DDSL –** Designated Deputy Safeguarding Lead
- **CPG –** Child Protection Governor
- **LADO –** Local Authority Designated Officer
- **ERSCP –** East Riding Safeguarding Children Partnership
- **CST –** Local Children Safeguarding Teams
- **Front Door –** Safeguarding and Partnership Hub
- **DBS –** Disclosure and Barring Service (formerly CRB)
- **KCSiE –** Keeping Children Safe in Education 2023 Statutory Guidance
- **EWO/S –** Education Welfare Officer/Service
- **YFS –** Youth & Family Support
- **PET –** Prevention & Education Team
- **Safeguarding** refers to the protection, safety and promotion of the welfare of all pupils/pupils and students including when in offsite provision or activities and using IT. This includes the building of resilience and awareness of risk through the formal and informal curriculum.
- **Child –** Any pupil under the age of 18 is legally a child.
- **Pupils/pupils and students 18 or over** If there is a concern about the welfare of a pupil aged 18+ DSL/Deputy DSL are advised to seek advice in the same way as with children. E.g. Front Door may signpost to Adult Services or refer to YFS. Please also see section 21 in respect of staff pupil relationships.

Contents

Safeguarding and Online Safety – Designated People and Advice Contact List

Child Protection – Designated People and Advice Contact List

Designated Safeguarding and Online Safety Lead	**Woldgate** Helen Handley (DSL) Claire Wright (DDSL) **Stamford Bridge** Nicola Massey (DSL) Lewis Horrocks (DDSL) **Pocklington** Kelly Foxton (DDSL) Kirsty Whitworth (DSL) **Melbourne** Victoria Burdett (DSL) Rebecca Winlow (DDSL)	**Woldgate (01759) 302395** hhandley@woldgate.net cwright@woldgate.net **Stamford Bridge (01759) 371430** nicolamassey@stamfordbridgeschool.co.uk lewishorrocks@stamfordbridgeschool.co.uk **Pocklington (01759) 302224** kelly.foxton@pocklingtonjuniors.co.uk kirsty.whitworth@pocklingtonjuniors.co.uk **Melbourne – (01759) 318369** vburdett@mcps.org.uk rwinlow@mcps.org.uk
Headteacher/Head of School	Luke Sloman (WG) Nicola Massey (SB) Vicky Burdett (M) Kelly Foxton (PJS)	(01759) 302395 (01759) 371430 (01759) 318369 (01759) 302224
Child Protection Governor	Patrick John (WG) Gill Faulkner (WG) Chris Leng (SB) Sandra Burley (P) Rebecca Major (M)	(01759) 302395 (01759) 302395 (01759) 371430 (01759) 302224 (01759) 318369
Chair of Governors	Patrick John (WG) Roddy Vann (SB) Sandra Burley (PJ-Acting) Jane Henley (M)	(01759) 302395 (01759) 372140 (01759) 302224 (01759) 318369
WLP Safeguarding Trustee	John Sinclair	(01759 302395)
Chair of Trustees	Graham Cook	(01759) 302395
WLP Safeguarding Lead	TBC	
Front Door (Safeguarding and Partnership Hub) Early Help Service	**CP initial referral** **Support & Advice:** Intensive & Specialist Safeguarding support Urgent C P concerns Consultation with Social Worker	**Mon to Thu** 8:30am – 5:00pm **Fri** 8:30am – 4:30pm **01482-395500** Request for Service (RFS) forms to: **safeguardingchildrenshub@eastriding.gov.uk**

Children's Emergency Duty Team	Urgent CP concerns outside of office hours where a child is at risk of significant harm.	01482 393939
Early Help Locality Hub	**Early Help** Additional Support for children & family's initial consultation	Consultation 01482 391700 Request for Service form to the Hub nearest to where the child lives. ehp.wolds@eastriding.gov.uk
Local ER Children Safeguarding Team	Wolds and Dale SCT	(01482) 392370
ER Child Protection Officer & LADO (Schools)	For CP & safeguarding advice & referral of allegations	LADO@eastriding.gov.uk Jayne.hammill@estriding.gov.uk (01482) 396999
School critical incident & Educational Visits Emergencies (not CP)	24-hour guidance and support	(01482) 392999
Humberside Police	ER Protecting Susceptible People Unit	01482 220809 / 220808 (County Hall, part of Front Door previously known as EHaSH)
ER Safeguarding Children Partnership	General strategic & Operational Safeguarding & CP advice	Tel (01482) 396994 erscp.enquiries@eastriding.gov.uk
East Riding Safeguarding Children Partnership	Training	(01482) 396994 erscp.training@eastriding.gov.uk
Prevent Referral	Humberside Police ERY LA	101 prevent@humberside.pnn.police.uk prevent@eastriding.gov.uk

1. Introduction

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

The Education and Inspectors 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 online-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 an end of electronic devices and the deletion of data.

In the case of both acts, action can only be taken over issues covered by the published Behaviour 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 take place out of school.

***2.* Roles and Responsibilities**

The Local Governing Committee (LGC) are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the LGC receiving regular information about online safety incidents and monitoring reports. The LGC will:

• regularly monitor online safety incident logs

• regularly monitor filtering/change control logs

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead (DSL).

The Headteacher and members of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The monitoring system used at Woldgate School is Senso Safeguard. This system uses artificial intelligence to monitor user keystrokes. It draws on a constantly updated database of flag words, phrases and acronyms to compare words, phrases and keystrokes. Where it identifies a potential concern, a screenshot is taken and the incident is logged. The DSL, DDSL and Network Manager have access to incident log, and this is monitored daily by the DDSL. A weekly report is also generated that is delivered to both the DSL and DDSL. Incidents are then reported on Safeguard and investigated as per the process outlined below.

More information about the Senso Safeguard system can be found here:

Safeguard Cloud Online Monitoring and Safeguarding - Senso Cloud

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

The Online Safety Lead will:

- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority where appropriate
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Deputy Designated Safeguarding Leads to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings

Designated Safeguarding Lead and Deputy Designated Safeguarding Lead

The DSL and DDSL training include online safety issues and awareness of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers

- potential or actual incidents of grooming
- online-bullying

On a day-to-day basis, the DDSL monitors alerts from the filtering and monitoring software, and investigates reports from staff or the monitoring system as to potential misuse.

Technical Support Staff

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority/HAD safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies and emails are regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior
- Leaders for investigation/action/sanction
- that monitoring software/systems are implemented and updated as appropriate.

Teaching and Support Staff

Teaching and Support staff have a responsibility to ensure that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood, and accept the staff acceptable use policy (in the Safeguarding and Child Protection policy)
- they report any suspected misuse or problem to the DDSL via the normal Safeguarding reporting system for investigation/action/sanction.
- all digital communications with pupils and students/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils and students understand and follow the Online Safety Policy and acceptable use policies
- pupils and students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils and students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils

Pupils are responsible for using the school digital technology systems in accordance with the student acceptable use agreement:

- they have read, understood, and accept the acceptable use agreement (included in the Home/School Agreement)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records
- their children's personal devices in the school (where this is allowed)

3. The Policy

Education -Pupils and students

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils and students to take a responsible approach. The education of pupils and students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum provided as part of the Personal Development and Computer Science curriculums
- Key online safety messages reinforced as part of a planned programme of assemblies
- Pupils and students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils and students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils and students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils and students should be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils and students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils and students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

It is accepted that from time to time, for good educational reasons, pupils and pupils and students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:
• Curriculum lessons
• Newsletters, website and ClassCharts Announcements and reminders, including links to useful websites
• Parents/carers evenings
• High profile events/campaigns e.g. Safer Internet Day

Education and Training – Staff

It is essential that all staff should receive online safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of the induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The Online Safety Lead will receive regular updates through attendance at external training events and National College training and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to staff in staff meetings or training
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Technical Infrastructure, Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The administrator passwords for the school systems, used by the Network Manager must also be available to the Headteacher or another nominated senior leader and kept in a secure place
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and those regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored

- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- The school has provided enhanced user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. ITTs, ECTs, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff/pupils and students) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the
- internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Devices

Any mobile phones brought into the school are done so at the pupil's own risk.

The aims of the mobile phone policy are:

1. To ensure that all classrooms are learning spaces, that avoids distractions from mobile phones
2. To safeguard pupils and staff from inappropriate use of mobile phones, including filming and photographing
3. To make sure that pupils are not walking around whilst using mobile devices and therefore reducing safety hazards

For pupils in Years 7 to 11, if brought to school, mobile phones must remain out of sight and switched off or on silent at all times. For Sixth Form pupils and students, mobile phones may only be used in the Sixth Form Study Room or Common Room.

Consequences for pupils not following the above policy:

- Staff will confiscate the mobile phone and it will be handed into the Inclusion Room
- If it is proved that a pupil has used his/her phone to bully or intimidate another person, the phone will be confiscated and returned only to a parent/carer. The school will then decide on the appropriateness of that pupil having a mobile phone in school following such an incident.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

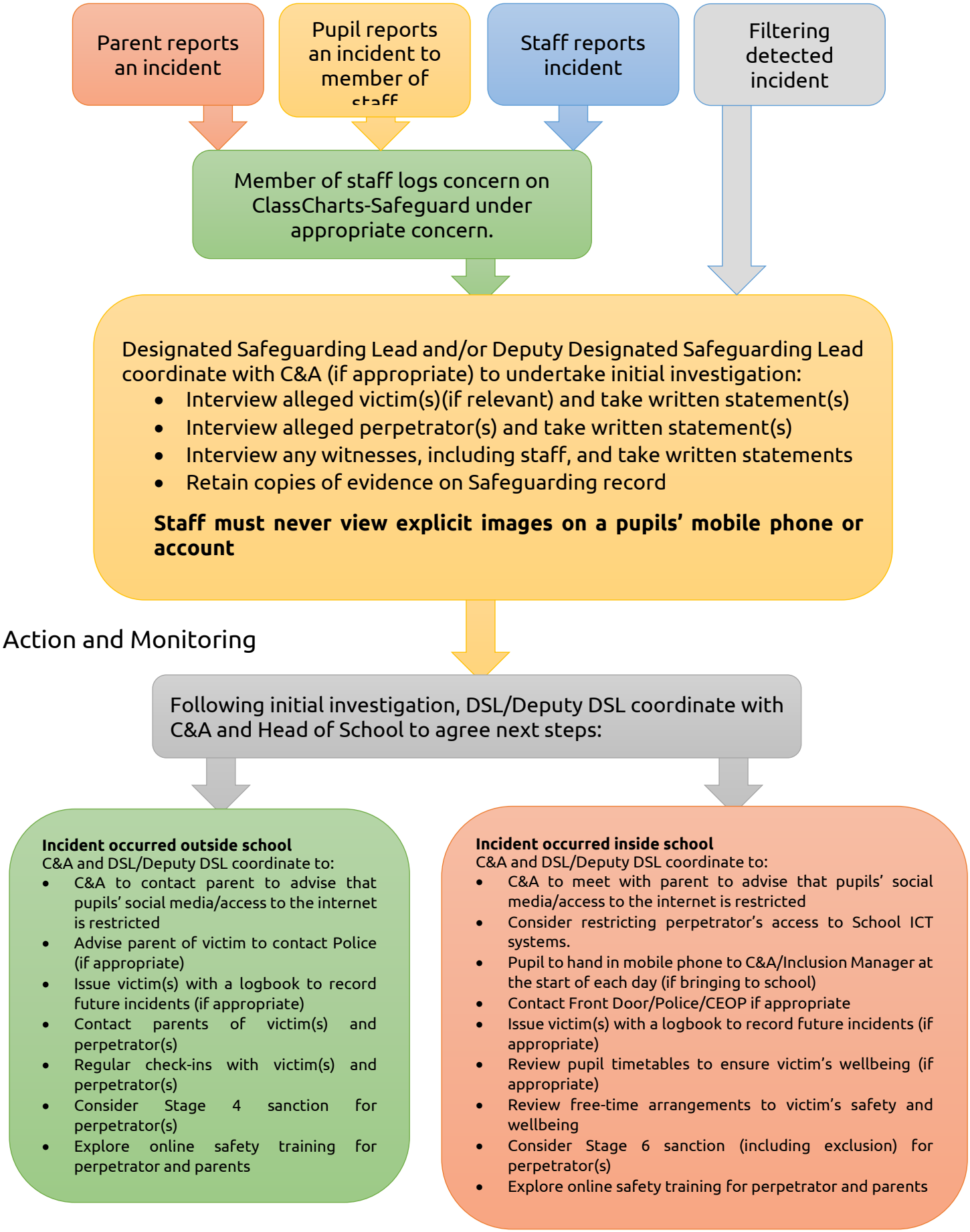
- When using digital images, staff should inform and educate pupils and students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils and students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images to ensure that pupils and students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils and students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils and students will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils and students' full names will not be used anywhere on a website or blog, particularly in association with photographs without prior consent being obtained.

Communication

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils and students or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils and students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Online Safety Incident Reporting



Online Safety in the Curriculum

All pupils and students at Woldgate School will receive an on-going online safety education programme. This programme will inform pupils and students of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments as new technology is adopted. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

The Computer Science department and Personal Development department have collaborated to run an ongoing programme covering all aspects of e-Safety.

The content is regularly reviewed to include up to date issues and is developed in line with DfE guidance and covers:

Content Risks:
Identifying fake content
Risks associated with social media (violence, hate speech, pornography, etc.)

Contact Risks:
Grooming
Image sharing
Scams

Conduct Risks:
Web archiving & Digital footprints
Bullying
Obsession & Self Image

Currently this includes:

Year 7
E-Safety (including grooming)
Online bullying

Year 8
Responsible use of the internet / digital tattoo
Online gaming
Grooming

Year 9
Sexting & Sexual Exploitation Online – Year 9
Identifying fake / untrustworthy content
Image sharing
Obsession & Self Image

Year 10 and 11
Sharing images
Digital behaviour and footprint
Online sexual harassment
Impact of pornography

Sixth Form

Our Sixth Form College ensures that there is a robust Online Safety education programme within the Sixth Form curriculum, and that the Care & Achievement team are up to date with the issues within their area.

The online safety education programme will be delivered through the Post-16 Personal Development programme.

The SENCO will work to ensure that there are accessible and adequate resources available for SEND pupils and students of the school to access the same online safety education as the rest of the school.

The PSHE and Personal Development curriculum will be regularly reviewed to ensure that it has appropriate and relevant online safety content incorporated into its programme.