Glebe Junior School

Online Safety and Acceptable Use of IT Policy

Date	Approved by	Minute Number
11 December 2023	Full Governors	FGB08/12/23 – new policy

Contents

1. Introduction

This Online Safety Policy outlines the commitment of Glebe Junior School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This policy applies to all members of Glebe Junior School (including staff, governors, supply teachers, volunteers, contractors, 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, or who use technology in their school role.

What is this policy?
Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents: It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures. Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022). These provide a helpful approach to understand the risk and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all four.

This policy works alongside the following school policies and documents:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Data Protection Policy
- Social Media Policy
- Bring your own Device Policy
- Staff Code of Conduct
- Derbyshire LA Acceptable Use of IT: Advice and Guidance.

2. Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

Headteacher and Senior Leaders:

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as

defined in Keeping Children Safe in Education.

- The headteacher and (at least) another member of the senior leadership team should be 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 is responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

- The headteacher/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.

- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)

- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments

- have a leading role in establishing and reviewing the school online safety policies/documents

- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond

- liaise with curriculum/year group leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

- provide (or identify sources of) training and advice for staff/governors/parents/carers/ learners liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)

- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to a DSL for investigation/ action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are 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
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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*
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Governing Body

- 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 (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- "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." In-line with 'Teaching Online Safety in Schools 2019' and the UKCIS cross- curricular framework 'Education for a Connected World' 2020 to support a whole-school approach.

IT Service Provider

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in school policies

Pupils

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else
- 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
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher
- 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 and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images etc
- dedicated page on school website with information about national/local online safety campaigns and literature, guidance to support parents at home. Information about high profile events and reference to web sites such as saferinternet, swgl, internetmatters

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.

3. Education and Curriculum

We have established a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stages of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, 'Teaching Online Safety in Schools' recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils. The following subjects have the clearest online safety links:

- PSHE including Relationships education and health education and citizenship
- Computing

We follow the NCCE Teach Computing scheme for our computing lessons and supplement this using Project EVOLE which incorporates the 'Education for a Connected World' framework which includes:

- Self-image & identity
- Online relationships
- Online reputation
- Copy right
- Ownership
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security

We recognise that online safety and broader digital resilience must be thread throughout the curriculum It is the role of 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 are doing and consider potential dangers and the age appropriateness of websites.

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g., disinformation, misinformation and fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law.

4. 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 and PSHE.) General concerns must be handled in the same way as any other safeguarding concern.

School procedures for dealing with online safety is detailed in the Child Protection & Safeguarding policy as well as the Behaviour & Anti-Bullying Policy.

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 or during extended periods away from 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 DSL on the same day. 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 Chair of Governors 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).

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.

if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include:

- Non-consensual images
- Self-generated images
- Terrorism/extremism
- Hate crime/ Abuse
- Fraud and extortion
- Harassment/stalking
- Child Sexual Abuse Material (CSAM)
- Child Sexual Exploitation Grooming

- Extreme Pornography
- Sale of illegal materials/substances
- Cyber or hacking offences under the Computer Misuse Act
- Copyright theft or piracy

See Appendix A for flowchart detailing and summarising action needed to be taken for different online safety incidents.

5. Filtering and Monitoring

Keeping Children Safe in Education 2023
"Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks. "

The school has an external technology provider (Lead IT Services). Working with the Senior Leadership Team (DSLs) and Governors as part of an Online Safety Group, they ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures are implemented in accordance with the Filtering and Monitoring Standards identified in Keeping Children Safe in Education 2023:

1: System Management
2: Review Provision
3: Restricted Content
4: Monitoring Strategy

Persons Responsible
Steve Watson – Headteacher – Senior DSL
Vicky Spender – Deputy Headteacher – DSL – SLT Member responsible for Filtering and Monitoring
Rachel Whelpton – Assistant Headteacher – DSL – SLT – SENDCO
Sophie Titmus – Assistant Headteacher – DSL – SLT
Samantha Finlayson – Assistant Headteacher – DSL – SLT

Filtering System: Iboss

- The school filtering system is reviewed and updated in response to changes in technology and patterns of online safety and incidents/behaviours
- The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre 'Appropriate Filtering For Education Settings'
- Access to online content and services is managed for all users

- Illegal content is filtered by the filtering provider by actively employing the IWF CAIC list and the police assessed list of unlawful terrorist content, produced by the Home Office. Content lists are regularly updated
- There are established and effective routes for users to report inappropriate content
- There is a process in place to deal with requests for filtering changes
- The system has differentiated user level filtering
- Filtering logs are reviewed regularly and alert the school to breaches which are then acted upon
- If necessary, the school will seek advice from, and report issues to, the SWGfL 'Report Harmful Content site

Monitoring System: Senso

- Senso is the system used to monitor network use across devices and services
- Users are aware that the network is being monitored
- There is a staff lead responsible for managing and monitoring strategy and processes (Vicky Spender)
- There are effective protocols in place to report abuse/misuse. There is a process for prioritising response to alerts that require rapid intervention. Management of safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon

The school follows the UK Safer Internet Centre 'Appropriate Monitoring For Schools' guidance and protects users and school systems through the use of the appropriate blend of strategies:

- Physical monitoring (adult supervision in the classroom)
- Internet use logged, monitored and reviewed
- Filtering logs are regularly analysed and breaches reported to SLT

6. Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the acceptable use agreements:
Appendix B: Learner's Acceptable Use Agreement
Appendix C: Parents and Carers' Acceptable Use Agreement

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- Pupil starter pack
- Staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

a) **Misuse of school technology**

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. 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.

b) Social Media

We have clear rules and expectations of behaviour for children and adults when using social media in our school community. Reference should be also be made to Social Media Policy and Derbyshire LA – Acceptable Use of IT: Advice and Guidance (Section 9) These are also governed by our school's Acceptable Use Policies and Staff Code of Conduct. Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

c) Electronic Communication

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a 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.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

d) Digital Images and Video

The school will inform and educate users about the risks associated with publishing images online and will implement policies to reduce the likelihood of the potential for harm

- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes – permissions can be found on Integris.

- 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 in 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 *learners* 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, storage, distribution and publication of those images
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website.
- they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

e) <u>Device Usage</u>

Personal devices including wearable technology and mobile telephones:

Pupils, who walk to or from school alone, are allowed to bring mobile phones into school. Mobile phones have to be turned off before arrival on school property and not turned back on until the pupil has left the school premises. Upon arrival in the classroom, pupils should hand in their mobile phone to their class teacher who will keep them in an allocated space. During the school day, phones must remain turned off at all times and pupils should not attempt to access these. Any attempt to use a phone in school will lead to an appropriate sanction. Pupils are not allowed to have wearable technology which links to the internet.

All staff who work directly with children should leave their mobile phones on silent and only use them when they not teaching or in direct contact with pupils. Child/staff data should never be downloaded onto a private phone. Smart watches including Fitbits are permitted to be worn by staff but to be used only as a watch when working with children. Therefore, other functions must be disabled when staff are with children.

Staff are not permitted to use personal laptops, memory sticks or external hard drives within school.

Volunteers, contractors, governors should keep their phones away and on silence during school hours. 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 should be sought from the site team or a member of SLT and this should be done in the presence of a member of staff during school hours.

Network/internet access on school devices:

Pupils are not allowed networked file access via personal devices. Pupils can access the school wireless internet network only via school technology and not using personal devices (which remain switched off during the school day).

Home devices are issued to some pupils. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked. The devices are filtered monitored when on home Wi-Fi connections.

Visitors, contractors, governors can access guest Wi-Fi which is subject to filtering. There is no access to the school's networks or files.

Trips / events away from school:

For school trips/events away from school, teachers will be able to use their personal mobile phone in an emergency or in any other communication with the school. Support staff and volunteers should not be using their mobile phones at any other time unless authorised by the teacher leading the trip.

f) User Accounts and Passwords

Every user within the school is given their own user account to allow access to the school network. Passwords for accounts must be secure, not easily guessed and kept private.

The minimum requirement for a password used with the schools ICT facilities should:

- be AT LEAST 6 characters long.
- Include a mixture of uppercase and lowercase letters
- Contain at least one number
- Not be easily guessable
- Changed periodically – this is currently enforced at 3 months.
- Never be written down
- Passwords for external sites must follow this same guidance (e.g. Accelerated reader, OTrack etc)

Users are not permitted to allow anyone to access their user accounts other than themselves. Computers are lockable by Windows + L. This facility should always be used while the computer is left unattended and logged in.

g) Locked Printing

All communal printers in school have the ability to securely store and lock print jobs for future release. This functionality must be used for any content which contains personal or confidential information. As a best practice locked print jobs should be used at all times.

h) Software, Copyright and Licensing

When a software product is purchased the purchaser does not 'own' the software but has only purchased the right to use the product in the ways defined by the copyright holder. In the United Kingdom, these rights and regulations automatically cover any original work. Copyright is part of a set of legal rights and regulations covering books, music, software and web-sites. Therefore, copyright and ownership of the software program remains with the copyright holder (normally the publisher) and is not transferred to the user. Licensing and copyright restrictions are important for ensuring that the creators of materials and resources are acknowledged and rewarded for their work, as well as ensuring that materials are used legally and without risk or prosecution. Licensing is the formal statement of what actions can and cannot be performed with a copyrighted resource.

Copyright law also applies to many aspects of Internet use. Users must ensure that the school either owns the copyright, or has written permission from the copyright holder, for any material that they intend to upload, or cause to be uploaded to the Internet or passed on my any electronic means to third parties. When downloading material, the school must observe any copyright statements that appear, or in the absence of any copyright statements, follow the normal practice as applied to printed materials. Unless otherwise stated on the site, any downloaded material must not be passed on to any third parties. Many sites are now classifying their resources with a Creative Commons (cc).

Rights and Responsibilities

- It is the responsibility of the school to ensure that all software is properly licensed.

- It is the responsibility of the Network Administrator and ICT coordinator to record and review software purchasing and licensing agreements and to ensure that all the members of the school community are informed of the licensing regulations governing the use of the school's software.

- It is the responsibility of the Network Administrator to install or deploy software onto computer systems and to keep and maintain software inventory lists.

- The certificates of authenticity must accompany the transfer of ownership of any computer to or from school that contains any of the Microsoft Operating Systems.

- The End User License Agreement (EULA) is supplied with the product's packaging or appears on the screen during the installation process. It is the responsibility of all members of the school community to observe the copyright regulations of each software product formally stated in the software license or EULA.

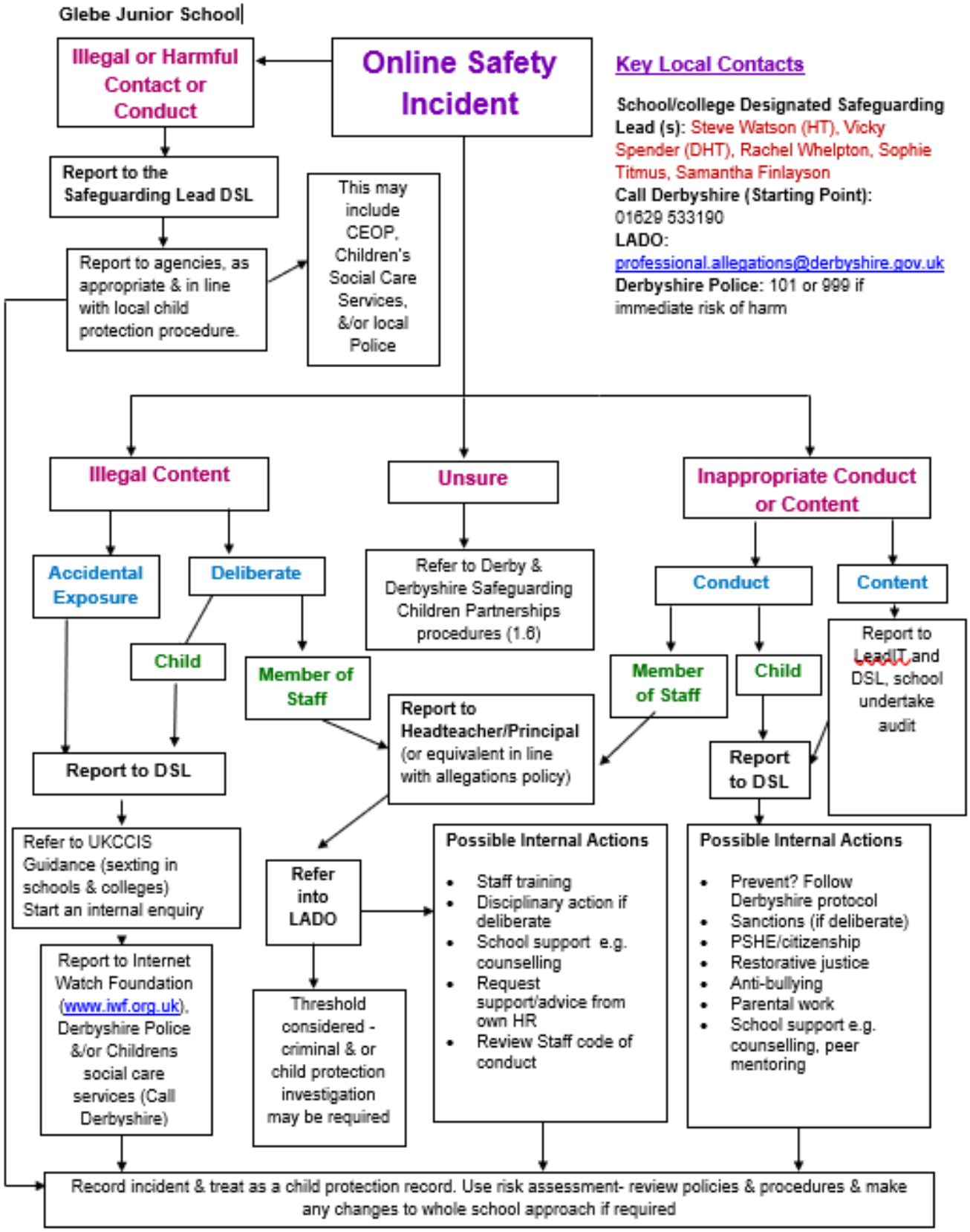
- It is the responsibility of all users to observe the copyright regulations and ensure that sources are acknowledged when copying material from the internet.

- It is permitted for web browsers and proxy servers to make temporary copies of web pages or relevant files (caching), as it is integral to accessing the internet and using it efficiently. Temporary copies of files or web pages for the purpose of electronic transmission such as email, to an individual for their private study or research are also permitted. Individual computers automatically delete the 'Temporary Internet Files' at logoff.

- As with all photocopying, it is the responsibility of the user to ensure that they do not reproduce more than 1% of the web site. Reproducing a single copy of a web page is allowed for private study or research, providing it is not used for producing multiple copies or redistribution in paper form or electronically.

APPENDIX A

Incident Flowchart



Reformatted with kind permission from theeducation people, Online Safety Education Advisor, www.kesi.org.uk

Version 3 - 2020/21. DP CPM Schools/Education

04/12/2020

APPENDIX B

Pupil Acceptable Use Agreement

This agreement will help me to keep safe online, make sure I use school devices responsibly and understand good online behaviours.

For my own personal safety:

- ✓ I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- ✓ I will only use devices, sites, apps and games that trusted adults have told me are safe to use.
- ✓ I will keep my username and password safe and secure and not share it with anyone else.
- ✓ I will only communicate online with people I have met in real life or that a trusted adult knows about.
- ✓ I will not share personal information about myself or others when online.
- ✓ I will immediately tell an adult if I see anything or anything happens which makes me feel uncomfortable online.

I will look after the devices I use, so that the school and everyone there can be safe:

- ✓ I will use the school internet and devices for schoolwork and other activities to learn and have fun with permission from an adult.
- ✓ I will handle all the devices carefully and only use them if I have permission.
- ✓ I will not try to alter the settings on any devices or try to install any software or programmes.
- ✓ I will tell an adult if a device is damaged or if anything else goes wrong.

I will think about how my behaviour online might affect other people:

- ✓ When online, I will act as I expect others to act toward me.
- ✓ I will not copy anyone else's work or files without their permission.
- ✓ I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- ✓ I will not take or share images of anyone without their permission.
- ✓ I will not share anything that I know another person wouldn't want shared, or put anything online which might upset other people.

I know that there are other rules that I need to follow:

- ✓ If I have a mobile phone in school, I will turn it off and hand in to my teacher at the start of the day and will not switch it on or use it on school grounds.
- ✓ Where work is protected by copyright, I will not try to download copies (including music and videos).
- ✓ When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful.
- ✓ I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- ✓ I know that I am expected to follow these rules in school and that I should behave in the same way out of school.
- ✓ I understand that if I do not follow these rules, it may lead to school taking action.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Class: ..... Date: .....

APPENDIX C

Parent/Carer Acceptable Use Agreement

Glebe Junior School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Child Protection policies which can be found on the school website. We attempt to ensure that all pupils have good access to digital technologies to support their learning and we expect our pupils to agree to be responsible users to help keep everyone safe and to be fair to others.

Your child will be asked to read and sign a Pupil Acceptable Use Agreement. This will be explained to all learners to ensure that they understand. Please read this carefully for your own information. It can be found in the Online Safety and Acceptable Use of IT Policy on our website.

As a parent/carer, please read the following Acceptable Use for Parents/Carers and sign.

Name of Child:

I am agreeing to:

- ✓ I understand my child's school uses technology as part of daily life of the school and give my child permission to use the internet at school and the school's digital devices and equipment.
- ✓ I accept that school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
- ✓ I understand that the internet and device usage in school is subject to filtering and monitoring. This also applies to school devices used out of school.
- ✓ I will support the school by promoting positive, responsible and safe online behaviours in my own use of technology including social media. I will not share other's images or details without permission and I will refrain from posting negative or threatening comments about others including school staff, volunteers, governors, contractors, pupils or other parents/carers.
- ✓ I will follow the school's policy on digital images and video and I will not share images of other children (or staff) at school events online.
- ✓ I understand the school sometimes uses images for internal purposes and it will only do so publicly if I have given my consent.
- ✓ I understand whilst at home, networks are much less secure than at school and I can apply child safety settings to my home internet. (Internet matters.org provides guides to do this easily for all the main internet providers in the UK)
- ✓ I am aware that that parental controls and settings can be applied to many different digital devices (Detailed information and guidance can be found on Internetmatters.org for all smart phones, gaming devices, etc.)
- ✓ I understand that for my child to grow up safe online, they will need positive input from school and home, so I will talk to my child about online safety.
- ✓ I understand and support the commitments made by my child in the Pupil Acceptable Use Agreement which they have signed and I understand they will be subject to the school's Behaviour Policy if they do not follow these rules.
- ✓ I can talk to my child's class teacher or a member of the Senior Leadership Team if I have any concerns about my child's use of technology, or about that of other members of the school community, or if I have questions about online safety or technology in school.

I/We have read, understood and agreed to this Acceptable Use.

Signed_____ Print Name_____ Date_____