Contents

# Hallgate Primary School

# Online Safety Policy

Date created: [08/12/22]

Next review date: [00/00/00]

# Scope of the Online Safety Policy

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

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Hallgate Primary 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.

# Policy development, monitoring and review

This Online Safety Policy has been developed by Computing Lead in consultation with:

- *headteacher/senior leaders*
- *Designated Safeguarding Lead (DSL)*
- *Online Safety Lead (OSL)*
- *staff – including teachers/support staff/technical staff*
- *governors*
- *parents and carers*
- *the school council*
- *community users*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

# Schedule for development, monitoring and review

| | |
|---|---|
| This Online Safety Policy was approved by the *school governing body on:* | *15/03/23 Behaviour and Safety Committee* |
| The implementation of this Online Safety Policy will be monitored by: | *Headteacher, Designated Safeguarding Lead (Mrs C Shiels)*<br>*Deputy DSL, Online Safety Lead (Mr J Shephard)*<br>*Computing Lead (Mr M Easton)*<br>*and the associated Governors.* |
| Monitoring will take place at regular intervals: | *Annually* |
| The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *Annually* |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | *September 2023* |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | *East Riding Safeguarding / Data Protection teams*<br>*Police*<br>*Chair of Governors*<br>*Primarytech* |

# Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents (CPOMs) using the e-safety incident tag*
- *monitoring logs of internet activity (including sites visited) via securly*
- *internal monitoring data for network activity via securly*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Policy and leadership

# 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 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 may be delegated to the Online Safety Lead (at Hallgate Primary School this will be 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/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, 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 receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead. These will be shared with the governor as part of the Behaviour and Safeguarding Committee work plan.
- 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.

## Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g.by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the Behaviour and Safeguarding Committee whose members will receive regular information about online safety incidents and monitoring reports. The Chair of the Behaviour and Safeguarding Committee will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- *membership of the school Online Safety Group*

The governing board will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

## Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

## Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
- 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
- receive reports of online safety incidents and create a log of incidents 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 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 (see flow diagram on page 19 under the heading Reporting and Responding) and the need to immediately report those incidents using CPOMs and using the e-safety tag.
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners together with the computing Lead
- liaise with 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

## Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme using ProjectEVOLVE.

This will be provided through:

- a discrete programme (ProjectEvolve)

- PHSE and SRE programmes (Jigsaw)
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

## 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 Chrisse Shiels (Headteacher) or John Shepherd (Deputy Headteacher) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems. At Hallgate Primary School these include communication via Google Classroom, School email and ScholarPack.*
- 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 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have 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.

## IT Provider

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- 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 the local authority
- 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 to Designated Safeguarding Lead and Online Safety Lead 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 (see appendix 'Technical Security Policy).
- monitoring software/systems are implemented and regularly updated as agreed in school policies using the software Securly supported by PrimaryTech

## Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- 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 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 and requiring parents/carers to sign a copy which is held by the school.
- publishing information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc. This is covered by our Data Protection Policy
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school and appropriate use at home

### Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

*The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.*

## Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. At Hallgate this will include the members of the safeguarding group. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group has the following members:

- Online Safety Lead
- Designated Safeguarding Lead
- senior leaders
- online safety governor
- technical staff
- teacher and support staff members
- learners
- parents/carers

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs,
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

An Online Safety Group terms of reference template can be found in the appendices.

## Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

# Policy

## Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is annually reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and is accessible through Google Drive, Curriculum Policies
- is published on the school website.

# Acceptable use

## Acceptable use agreements

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

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | **Any illegal activity for example:**<br>• Child sexual abuse imagery*<br>• Child sexual abuse/exploitation/grooming<br>• Terrorism<br>• Encouraging or assisting suicide<br>• Offences relating to sexual images i.e., revenge and extreme pornography<br>• Incitement to and threats of violence<br>• Hate crime<br>• Public order offences - harassment and stalking<br>• Drug-related offences<br>• Weapons / firearms offences<br>• Fraud and financial crime including money laundering<br><br>N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges | | | | | X |

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)<br>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices<br>• Using penetration testing equipment (without relevant permission)<br>N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here | | | | | X |
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs) | | | X | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | Using school systems to run a private business | | | | X | |
| | Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | X | |
| | Infringing copyright | | | | X | |

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| | Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | X | X | |
| | Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |

| Consideration should be given for the following activities when undertaken for non-educational purposes:<br><br>Schools may wish to add further activities to this list. | Staff and other adults | | | | Learners | | | |
|---|---|---|---|---|---|---|---|---|
| | Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission/awareness |
| Online gaming | | | X | | X | | | |
| Online shopping/commerce | | | X | | X | | | |
| File sharing | | X | | | | | X | |
| Social media | | | X | | X | | | |
| Messaging/chat | | | X | | X | | | |
| Entertainment streaming e.g. Netflix, Disney+ | | | X | | X | | | |
| Use of video broadcasting, e.g. YouTube, Twitch, TikTok | | | X | | X | | | |
| Mobile phones may be brought to school | | X | | | | | | X |
| Use of mobile phones for learning at school | | | X | | X | | | |
| Use of mobile phones in social time at school | | | X | | X | | | |
| Taking photos on mobile phones/cameras | X | | | | X | | | |
| Use of other personal devices, e.g. tablets, gaming devices | | | X | | X | | | |
| Use of personal e-mail in school, or on school network/wi-fi | | | X | | X | | | |
| Use of school e-mail for personal e-mails | X | | | | X | | | |

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, social media, learning platform, etc.) 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 Mrs Shiels or another member of the SLT – 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. Depending on the type of communication these might need to be reported to PrimaryTech, Schools IT and the East Riding Safeguarding and Data Protection teams.
- 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.

# Reporting and responding

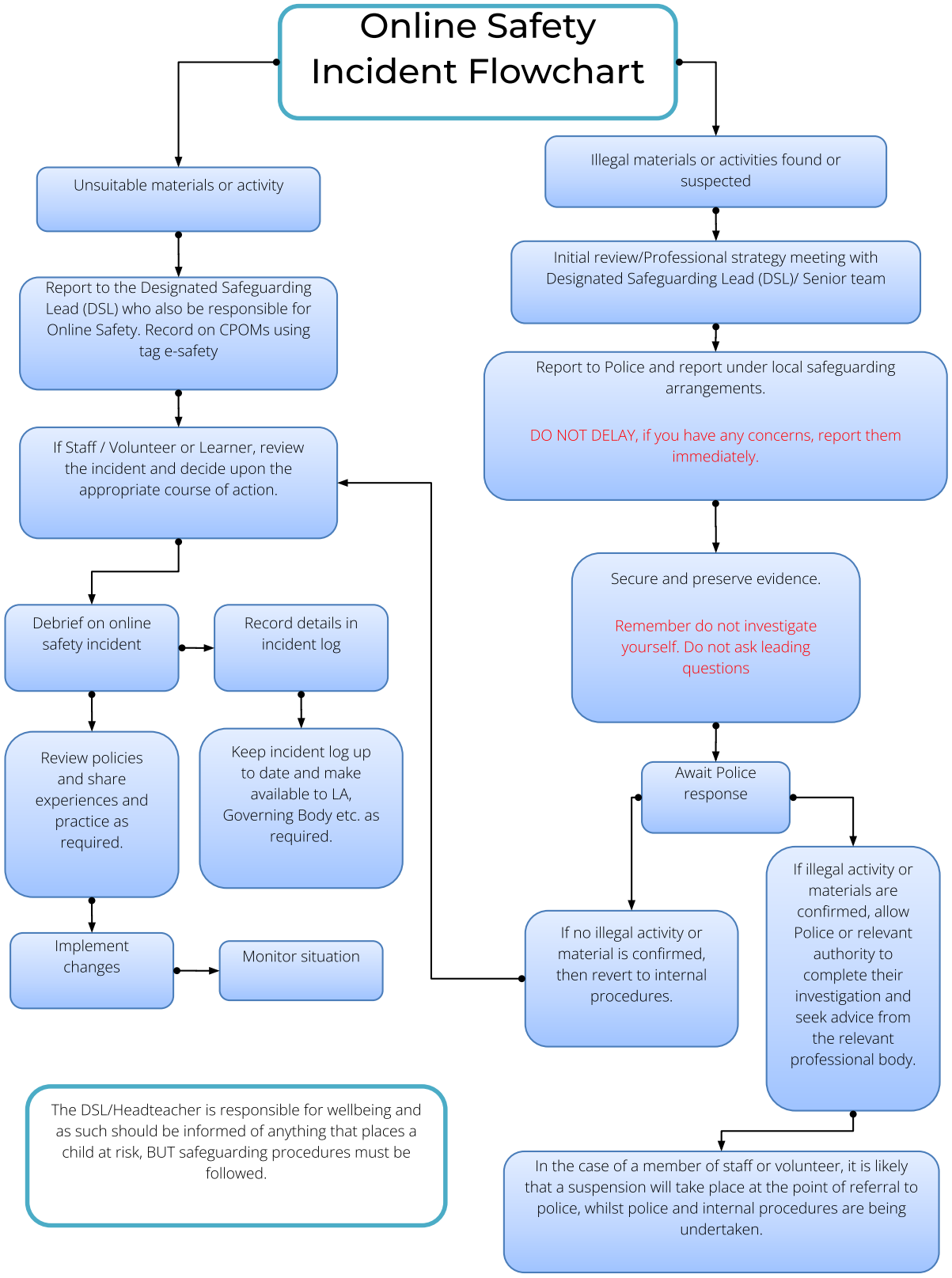
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. For staff they are to report using CPOMs using the appropriate tag(s). Children are encouraged to tell a member of staff if they have any concerns and these are dealt with according to the Safeguarding Policy.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead and Online Safety Lead have appropriate skills and training to deal with online safety risks, all staff have the responsibility to highlight training requirements
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), 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
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority. The Local Authority Designated Officer (LADO) will be contacted in the case of safeguarding concerns.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - at least 2 senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged using CPOMs if it involves children
- Incidents involving adults linked to staff should be reported to the Headteacher
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.

- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings at staff meetings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who also be responsible for Online Safety. Record on CPOMs using tag e-safety
If Staff / Volunteer or Learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review policies and share experiences and practice as required.
Keep incident log up to date and make available to LA, Governing Body etc. as required.
Implement changes
Monitor situation
Illegal materials or activities found or suspected
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

## School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

# Responding to Learner Actions

| Incidents | Refer to class teacher /tutor | Refer to Deputy Head | Refer to Headteacher | Refer to Police/Social Work | Refer to local authority technical support for advice/action | Inform parents/carers | Remove device/ network/internet access rights | Issue a warning | Further sanction, in line with behaviour policy |
|---|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities). | | X | X | X | | | | | |
| Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords | | X | X | | | X | | X | X |
| Deliberately corrupting or destroying the data of other users. | | X | X | | | X | | X | X |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | | X | X | X | X |
| Unauthorised downloading or uploading of files or use of file sharing. | X | X | X | | X | | | | |
| Using proxy sites or other means to subvert the school's filtering system. | | X | X | | X | X | | X | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident. | X | X | X | | X | X | X | X | X |
| Deliberately accessing or trying to access offensive or pornographic material. | X | X | X | X | X | X | X | X | X |

| Incidents | Refer to class teacher /tutor | Refer to Deputy Head | Refer to Headteacher | Refer to Police/Social Work | Refer to local authority technical support for advice/action | Inform parents/carers | Remove device/ network/internet access rights | Issue a warning | Further sanction, in line with behaviour policy |
|---|---|---|---|---|---|---|---|---|---|
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act. | | X | X | | X | X | | | |
| Unauthorised use of digital devices (including taking images) | | X | X | | X | X | | | |
| Unauthorised use of online services | | X | X | | X | X | | | |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | | X | X | | X | X | | X | X |
| Continued infringements of the above, following previous warnings or sanctions. | | X | X | | X | X | | | X |

# Responding to Staff Actions

| Incidents | Refer to line manager | Refer to Headteacher/ Principal | Refer to local authority/HR | Refer to Police | Refer to LA / Technical Support Staff for action re filtering, etc. | Issue a warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities) | | X | X | X | | | | |
| Deliberate actions to breach data protection or network security rules. | | X | X | | X | | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | X | | | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | X | X | | | | |
| Using proxy sites or other means to subvert the school's filtering system. | | X | X | | | X | X | X |
| Unauthorised downloading or uploading of files or file sharing | | X | | | | X | X | X |
| Breaching copyright or licensing regulations. | | X | | | | X | X | X |
| Allowing others to access school networks by sharing username and passwords or attempting to access or accessing the school network, using another person's account. | | X | | | | X | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | | | X | X | X |
| Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers | | X | | | | X | X | X |
| Inappropriate personal use of the digital technologies e.g. social media / personal email | | X | X | | | X | X | X |
| Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner | | X | X | | | X | X | X |
| Actions which could compromise the staff member's professional standing | | X | | | | X | X | X |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | | X | | | | X | X | X |
| Failing to report incidents whether caused by deliberate or accidental actions | X | X | | | | X | X | X |
| Continued infringements of the above, following previous warnings or sanctions. | X | X | X | | | X | X | X |

# Online Safety Education Programme

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 (Based upon ProjectEvolve) for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner needs and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- 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 learners are guided to sites checked as suitable for their use. Processes are in place for dealing with any unsuitable material that is found in internet searches. (see reporting and responding)
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit

- it is accepted that from time to time, for good educational reasons, 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 should be able to request the temporary removal of 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. Request should be discussed with the Computing Lead and should be requested through the PrimaryTech IT fault reporting system so that the request can be tracked.
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes. Regular monitoring by the subject leader takes place to ensure the quality of the learning and outcomes that are reported to the Headteacher and Governing Body.

# Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is being developed and recognised through:

- *mechanisms to canvass learner feedback and opinion such as classroom feedback, questionnaires*
- *appointment of digital leaders whose minutes are shared with the Online Safety Group. These digital leaders are being developed through an Online Safety Club.*
- *learners contribute to the online safety education programme e.g. digital leaders leading lessons, assemblies for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *supporting with computing clubs and events*

# Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly and a record maintained and stored on ScholarPack.

- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings as part of the Health and Safety Section on the staff meeting agenda
- the Online Safety Lead together with the Online Safety and Computing Curriculum Lead will provide or seek advice/guidance/training to individuals as required.

# Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents
- Participation in assemblies and lessons linked to online safety

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security (at least at the basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

# Families

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant websites / publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority

## Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision through sharing access to training

# Technology

The school is 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. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection. Hallgate Primary School works with PrimaryTech to ensure the online safety and security measures are in place. A Data Protection Impact Assessment (DPIA) has been completed for this contract.

# Filtering and Monitoring

The school filtering policies are agreed by senior leaders, governors and PrimaryTech and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL/Online Safety Lead will have responsibility for safeguarding and online safety and PrimaryTech will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by PrimaryTech with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

# Filtering

- the school manages access to online content and services across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).
- filtering logs are regularly reviews and alert the DSL to breaches of the filtering policy, which are acted upon.
- *younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle*

- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site it will also seek advice from the LA.

# Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up by the DSL, acted on and outcomes are recorded by the DSL and logged by the class teacher as required upon CPOMS
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- use of Securly to filtering, monitor and report breaches.

# Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements (outlined by local authority):

- responsibility for technical security resides with the Headteacher who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by PrimaryTech and will be reviewed, at least annually, by SLT.
- a password policy and procedures are implemented.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices 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 workstations are protected by up-to-date endpoint (anti-virus) software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Claire Cruickshank together with the Computing Lead and Primarytech are responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider

- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).
- guest users are provided with appropriate access to school systems based on an identified risk profile.

# Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

| | **School devices** | | | **Personal devices** | | |
|---|---|---|---|---|---|---|
| | School owned for individual use | School owned for multiple users | Authorised device[1] | Student owned | Staff owned | Visitor owned |
| Allowed in school | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only | | | | No | **Yes** | **Yes** |
| No network access | | | | **Yes** | | |

## School owned/provided devices:

- *Google Chromebooks are allocated to all teaching staff.*
- *iPads allocated to teaching staff*
- *Google Chromebooks are accessible to Teaching Assistant to access information such as emails and planning*
- *Chromebooks and iPads which have been allocated to staff are to be used for work, They can be used in classrooms and used for educational purposes.*

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- all school devices are managed through the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how it is used allowed
- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

### Personal devices

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storge is be made available. (See mobile phone policy)
- use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

## Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

- guidance for learners, parents/carers
- compliance though Data Protection Policies and Procedures and East Riding of Yorkshire Council.

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

## Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours

## Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school

- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

The social media policy template provides more detailed guidance on the school's responsibilities and on good practice.

# Digital and video images

The school will inform and educate users about these risks and has a Digital and Video Policy in place to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- 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 (if allowed) on school devices. Personal devices must not be used.
- 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 *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

- care should be taken when sharing digital/video images that learners are appropriately dressed
- 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/social media. (see parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy and Photo Policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

# Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media (Twitter)
- Online newsletters

The school website is managed/hosted by PrimaryTech. The school ensures that Online Safety Policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learners work, images or videos are published, their identities are protected, and full names are not published.

*The school website provides information about online safety e.g. Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.*

*The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.*

# Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy and is supported by the Local Authority in its implementation
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. Procedures are in place to enable staff to work from home as a work laptop will be provided.

- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.
- The Personal Data Advice and Guidance is in the appendix of this policy to support good practice.

# Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- Online Safety (and related) Policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

## Appendix

Policy

- Acceptable Use Agreement Policy
- Computing Policy
- Responding to incidents of misuse - flowchart
- Record of reviewing devices/internet sites (responding to incidents of misuse)

Advice and Guidance

- Legislation from SWGfL 2022
- Personal Data Advice and Guidance

Useful website

Glossary of Gaming terms

https://swgfl.org.uk/topics/gaming/the-language-of-gaming-a-dictionary-of-terms/

Online safety and slang glossary terms

https://www.internetmatters.org/connecting-safely-online/helpful-social-media-safety-guides-and-resources/online-safety-glossary-of-terms/

- A8 - Harmful Sexual Behaviour Policy Template (new template added September 2022)
- C1 - Technical Security Policy Template (including filtering and passwords)
- C3 - School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation (new DfE guidance from September 2022)
- C4 - Mobile Technologies Policy Template (inc. BYOD/BYOT)
- C5 - Social Media Policy Template