NORTHGATE

High School

Online Safety Policy

Respect | Determination | Teamwork

Review period: Biennial

Review by: Mr J Tunaley

Date Reviewed: November 2023

Next Review: November 2025

Online Safety Policy

1. Responsibilities

1.1 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.

2. Headteacher and senior leader

2.1 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.

2.2 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.

2.3 The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, Principal of ICT Infrastructure and Services, 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.

2.4 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.

2.5 The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

2.6 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.

3. Governors

3.1 Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

3.2 Emma Lightfoot, Parent Governor, is the Online Safety Governor and will engage with the school DSL/Online Safety Lead by:

- Attending meetings with the DSL/Online Safety Lead;
- Receive updates on the number of online safety incidents;
- Being part of the Online Safety Steering Group;
- Report back to the governing body.

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

4. Designated Safeguarding Lead (DSL)

4.1 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 Principal of ICT Infrastructure and Services on matters of safety and safeguarding and welfare (including online and digital safety).

5. Online Safety Lead

5.1 The Online Safety Lead will:

- lead the Online Safety Group;
- 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 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, 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 (particuarly by learners) with regard to the areas defined In Keeping Children Safe in Education:
  - □ Content;
  - □ Contact;
  - □ Conduct;
  - □ Commerce.

6. Curriculum Leads

6.1 Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme

This will be provided:

- PHSE and RSE programmes;
- A mapped cross-curricular programme;
- assemblies and pastoral programmes;
- through relevant national initiatives and opportunities.

7. Teaching and Support Staff

7.1 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;
- they immediately report any suspected misuse or problem to the Headteacher 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;
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies;
- 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.

8. Principal of ICT Infrastructure and Services

8.1 The DfE Filtering and Monitoring Standards says:

“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”

“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”

“The IT service provider should have technical responsibility for:

- *maintaining filtering and monitoring systems;*
- *providing filtering and monitoring reports;*
- *completing actions following concerns or checks to systems.”*

“The IT service provider should work with the senior leadership team and DSL to:

- *procure systems;*
- *identify risk;*
- *carry out reviews;*
- *carry out checks.”*

8.2 The Principal of ICT Infrastructure and Services 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 guidance from 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 (insert relevant person) 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 template’ for good practice);
- monitoring systems are implemented and regularly updated as agreed in school policies.

9. Learners

9.1 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.

10. Parent and Carers

10.1 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, cloud services;
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- reinforcing the online safety messages provided to learners in school;
- the safe and responsible use of their children's personal devices in the school.

11. Community Users

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

12. Online Safety Steering Group

12.1 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.

12.2 The Online Safety Steering Group has the following members

- DSL and OSL;
- AHT responsible for learning support;
- AHT responsible for PSHE;
- AHT responsible for school compliance;
- AHT responsible for progress;
- Principal of ICT Infrastructure and Services;
- Online safety governor.

12.3 Members of the Online Safety Steering Group will assist the DSL/OSL 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, where possible;
- 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.

13. Professional Standards

13.1 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.

14. Acceptable Use

14.1 We have an acceptable use agreement that all staff are expected to adhere to. They have signed to confirm they understand the importance of following that agreement.

Click here to access our Acceptable Use Agreement

Click here to access our Staff Code of Conduct

15. Reporting and Responding

15.1 As a school we take all reasonable precautions to ensure online safety for all school users but we recognise that incidents may still occur inside and outside of school and these will need intervention. Northgate ensures that:

- there are clear reporting routes which are understood and followed by all members of the school community. These are consistent with the school safeguarding procedures and low level concern reporting;
- 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, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks;
- 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.
- 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.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
  - □ one or more 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;

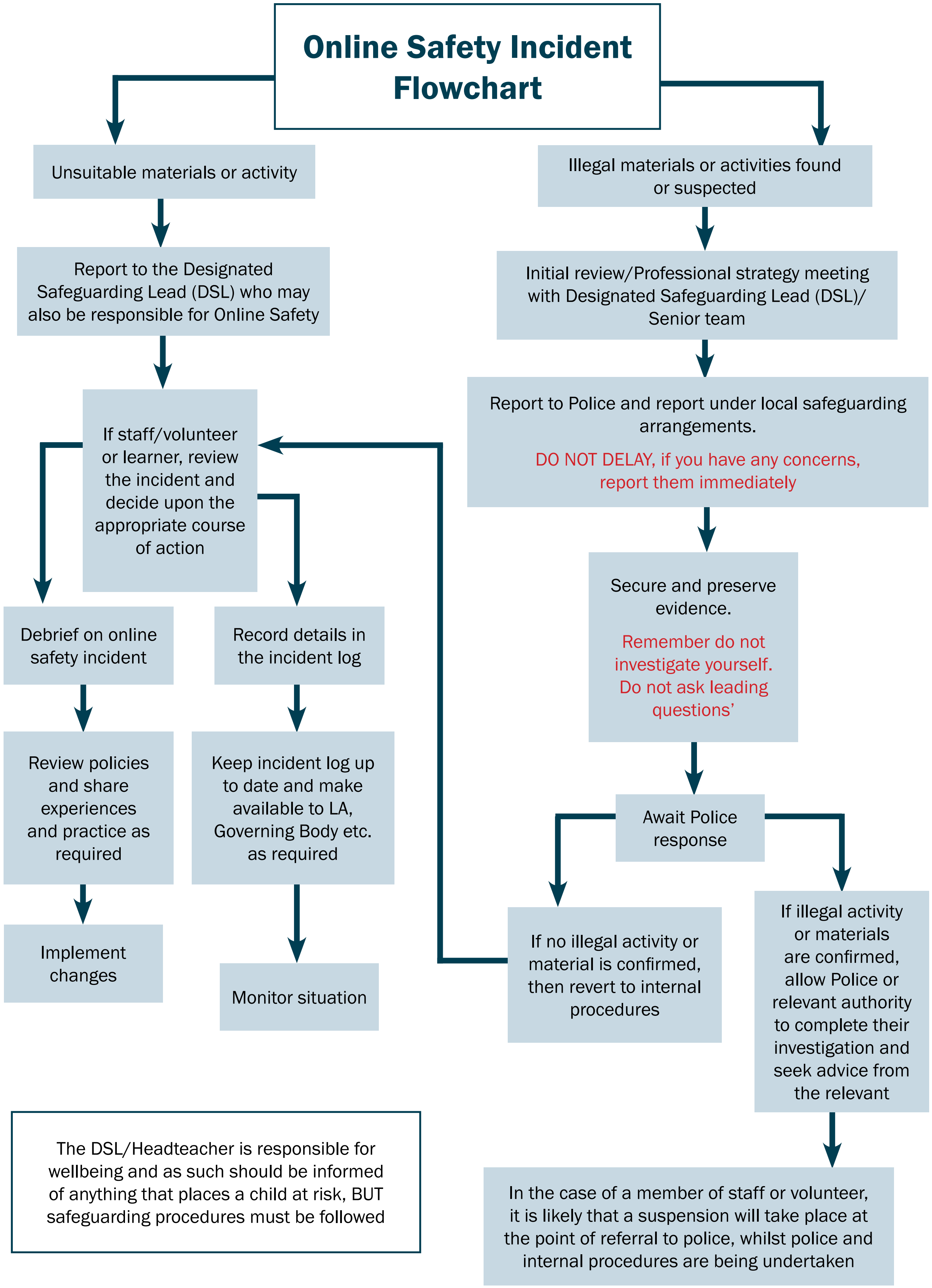
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively;
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident;
- all incidents are logged on CPOMS under cause for concern and ‘online safety issue’;
- 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;
    - learners, through assemblies/lessons;
    - parents/carers, through newsletters, school social media, website;
    - governors, through regular safeguarding updates.

16. School Actions

16.1 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.

16.2 **Click here to access our School Behaviour Policy.**

Online Safety Incident Flowchart



Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action

Debrief on online safety incident

Review policies and share experiences and practice as required

Implement changes

Record details in the incident log

Keep incident log up to date and make available to LA, Governing Body etc. as required

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

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

17. Online Safety Education

17.1 At Northgate we recognise the importance of giving our students the knowledge, understanding and skills required to navigate the online world safely. We know that is best done through preventative education.

17.2 Online safety is a focus for all teaching staff in all curriculum areas. Staff have been asked to plan opportunities to highlight the four Cs of internet safety. On top of that broad curriculum offer we deliver online safety education in the following ways:

- A planned online safety curriculum delivered through PSHE where lessons have been planned to meet the need, age range and prior learning of the students;
- Drop down days where there is a specific focus around online safety;
- Assemblies.

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

- 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;
- 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.

18. Families

18.1 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 etc;
- 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.

19. Technology

19.1 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.

20. Filtering and monitoring

20.1 The school filtering and monitoring provision is agreed by senior leaders, governors and the Principal of ICT Infrastructure and Services and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

20.2 Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the Principal of ICT Infrastructure and Services will have technical responsibility.

20.3 The filtering and monitoring provision is reviewed by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the Principal of ICT Infrastructure and Services.

20.4 Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided 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, and log, requests/approvals for filtering changes;
- filtering logs are regularly reviewed and alerts sent to the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon;
- the school has an acceptable use policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.

20.5 Monitoring

20.5.1 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, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored;
- 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.

20.5.2 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);
- filtering logs are regularly analysed and breaches are reported to senior leaders.

21. Technical Security

21.1 The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with SLT 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 the Principal of ICT Infrastructure and Services and will be reviewed, at least annually, by the SLT/Online Safety Group;
- password procedures are implemented;
- the security of their username and password and must not allow other users to access the systems using their log on details;
- 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 system will be protected by secure passwords. Passwords must not be shared with anyone;
- all administrator passwords for school systems require Two-Factor Authentication (2FA), where possible;
- 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 software;
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud;
- The Principal of ICT Infrastructure and Services is responsible for ensuring that all software purchased by and used by the school is adequately licenced 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;
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail);
- mobile device security and management procedures are in place;
- guest users are provided with appropriate access to school systems based on an identified risk profile.

22. Mobile technologies

22.1 The DfE guidance "Keeping Children Safe in Education" states:

"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy."

22.2 Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

22.3 All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

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

22.5 Northgate operates a on site, out of sight policy with regard to mobile technologies. Staff can allow students to use devices in lessons where it will improve learning outcomes.

22.6 **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;
- 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.

23. Social media

23.1 With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

23.2 Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

23.3 All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

23.4 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.

23.5 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'

23.6 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.

23.7 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.

23.8 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.

23.9 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.

24. Digital and video images

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

24.2 The school will inform and educate users about these risks and will implement policies 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 on school devices. The personal devices of staff should not be used for such purposes;
- 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;
- 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;
- 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.

25. Online Publishing

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

- Public-facing website;
- Social media;
- Online newsletters.

25.2 The school website is managed/hosted by the Network Manager. 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.

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

26. Data Protection

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

26.2 The school:

- has a Data Protection Policy;
- 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.

26.3 When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected;
- device will be password protected.

26.4 Staff must ensure that they:

- at all times take care to ensure the safe keeping 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 should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop 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.