WALTON AND LEES HILL CE PRIMARY SCHOOL

INTERNET SAFETY POLICY

Name: Lynn Rooney **Position:** Head Teacher **Next Review Date:** Sept 2025

THIS POLICY SHOULD BE READ IN CONJUNCTION WITH COMPUTING POLICY

Aims and Objectives:
We believe that the educational benefits of Internet access far outweigh the possible risks and that good planning and management will ensure appropriate and effective pupil use.

The purpose of Internet access in schools is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and an entitlement for pupils who need to show a responsible and mature approach. It should be noted that the use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

The school Online Safety Policy and procedures will help to ensure safe and appropriate use, and the development and implementation will involve all stakeholders in a child's education from the Head teacher and Governors to the senior leaders and classroom teachers, support staff, parents, carers, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk in and outside of school

The Internet can be used by pupils of all ages, by Teachers and by Governors to:
- Give access to world-wide educational resources including museums and art galleries
- Enable information and cultural exchanges between students world-wide
- Access news and current events
- Enhance cultural, social and leisure use in libraries, clubs and at home
- Promote staff professional development – access to educational materials and good curriculum practice
- Facilitate communication with the advisory and support services, professional associations and colleagues
- Exchange of curriculum and administration data with the Local Authority and the Department for Children Schools and Families

This school must demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The Online Safety Policy and procedures that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their families) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal, and recreational use.

Scope of Policy:

This Policy and procedures applies to all members of the School community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of our ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This includes incidents of cyberbullying (including prejudiced-based and discriminatory bullying), or other online safety related incidents covered by this Policy and procedures, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers in relation to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken in relation to issues covered by the published Behaviour Policy and procedures.

The school will deal with such incidents within this Policy and procedures and the Behaviour Policy and procedures which includes anti-bullying procedures.

Role of the Online Safety Governor and Governing Board:

The role of the Governors/online safety Governor is to:

- ensure a member of the Governing Body is elected to the role of Online Safety Governor *(Stewart Simpson) who* should then lead on relevant governance requirements below;
- ensure an appropriate senior member of staff from the School Leadership Team (SLT) is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety and an understanding of the filtering and monitoring systems and processes in place) with the appropriate status, authority, time, funding, training, resources, and support;
- ensure other roles and responsibilities are appropriately allocated to staff and third parties, e.g. external service providers in order to meet the DfE Digital and technology standards;
- ensure that systems are in place to meet the requirements of the DfE Cyber security standards. Schools must have a Cyber security and resilience strategy in place which is supported by an appropriate Cyber Response Plan;
- ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures;
- approve the Online Safety Policy and procedures, reviewing its effectiveness e.g. through Governors receiving regular information about online safety incidents and monitoring reports and making use of the UK Council for Internet Safety (UKCIS) guide Online safety in schools and colleges: Questions from the Governing Board;
- ensure that appropriate filters and appropriate monitoring systems are in place, but also consider how 'over-blocking' may lead to unreasonable restrictions on what pupils can be taught in relation to online teaching and safeguarding;
- ensure that the SLT and **all** staff have an awareness and understanding of the procedures and processes in place to manage filtering and monitoring and how to escalate concerns when identified;
- ensure all governors and trustees receive appropriate training on online safety which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring in relation to school owned IT devices;
- ensure that the school follows all current online safety advice to keep both pupils and staff safe;
- support the school in encouraging parents and the wider community to become engaged in online safety activities;
- have regular reviews with the Online Safety Coordinator/Designated Safeguarding Lead (DSL) and incorporate online safety into standing discussions of safeguarding at Governors meetings (including incident logs, adverse monitoring reports, change control logs etc.)

- ensure that where the online safety coordinator is not the named DSL or deputy DSL, there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety as a whole is not compromised;
- work with the Data Protection Officer (DPO), DSL and Head teacher to ensure a UK GDPR compliant framework for storing data, helping to ensure that child protection is always at the forefront and data protection processes support careful and legal sharing of information;
- check that school is making good use of information and support (Annex B – Further information which forms part of Keeping Children Safe in Education);
- ensure that all staff undertake regular updated safeguarding training, including online safety training, in line with advice from the Local Safeguarding Children's Partnerships (LSCP), and that it is integrated, aligned, and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning;
- recognise that a one size fits all educational approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed;
- ensure pupils are taught how to keep themselves safe, including online as part of providing a broad and balanced curriculum with clear procedures on the use of mobile technology.

The Role of the Head Teacher:

The Head teacher, who is also the DSL, has overall responsibility for online safety provision.

The Head teacher will:

- take overall responsibility for data and data security;
- foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding;
- ensure that the DSL responsibilities listed in the section below are being followed and fully supported;
- ensure that Policies and procedures are followed by all staff and other adults working paid or unpaid in the school;
- undertake training in offline and online safety, in accordance with statutory guidance and relevant Local Safeguarding Partnership recommendations;
- take responsibility for liaising with the Governors in order to achieve their obligations in meeting the DfE digital and technology standards, particularly as they relate to cyber security and filtering and monitoring and ensuring the Governors are regularly updated on progress towards the standards;
- ensure that online safety is appropriately monitored and reviewed by undertaking an annual review of the school's approach to online safety
- liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information;
- take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Governors to ensure a Data Protection Act 2018 (DPA) compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information;
- ensure the school implements and makes effective use of appropriate ICT systems and services
- be responsible for ensuring that **all** staff receive suitable training on induction to carry out their child protection and online safety roles (which should include the procedures and processes in place to manage filtering and monitoring and how to escalate concerns when identified).
- understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

- encourage parents/carers to provide age-appropriate supervision for children in their care using the internet including by the use of internet filters which should be used to block malicious websites (usually free but often need turned on.)
- ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including the risk of children being radicalised;
- take responsibility for formulating the school's Cyber security resilience strategy and Cyber response plan in liaison with the Online Safety Governor and other third party providers.
- ensure the school website meets statutory requirements.
- be aware of emerging online safety issues and legislation, and of the potential for serious child protection issues to arise from:

  - sharing of personal data;
  - access to illegal/inappropriate materials;
  - inappropriate online contact with adults/strangers; - potential or actual incidents of grooming;
  - cyberbullying and the use of social media.

Access to all web sites from school is automatically filtered managed by the schools' internet provider. Procedures are in place for senior staff to block and report inappropriate websites also. User settings are managed by Sensible Solutions who are the administrators for our server. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a terminal. Neither the school nor Cumberland Council can accept liability for the material accessed, or any consequences thereof although staff, parents, governors and advisors work together to establish agreement that every reasonable measure is being taken.

No personal data will be sent over the Internet by children without reference to his/her teacher and e-mail marked for individual children will be viewed first by the head teacher to ensure that it has come from a responsible source. Virus protection is installed and updated regularly.

Security strategies are managed in collaboration with Sensible Solutions.

The School Website:
Our school has created a website, to celebrate good work, gives details of events – past, present and future, to promote the school and provides links for the school with other organisations. Names and photos of pupils are never displayed together. We have sought parent's permission before using an image of their child. The Headteacher, staff and clerk to governors are responsible for updating the website, making sure that information displayed there is accurate and current.

Role of staff:
Internet access is a necessary part of planned lessons. It is an entitlement for pupils based on responsible use: At KS1, pupils will access teacher-prepared or chosen materials, rather than the open Internet. At KS2, pupils will access specific sites, or use search engines for specific tasks. Unsupervised access (ie during playtimes) is not allowed.

All reasonable efforts will be made to ensure copyright laws will not be infringed. Materials copied from the internet both by staff and pupils will be in accordance with the licence taken out by the LA.

Staff will monitor the value and credibility of web-based materials in relationship to other media as part of our topic based approached to the curriculum and will supervise pupils using the Internet appropriately.

Pupils will be taught to :

- validate information before accepting it as true.
- observe copyright when copying materials from the web.
- be aware that the writer of an e-mail or the author of a Web page may not be the person they claim to be.

At present only contact with other primary schools and approved educational institutions is allowed in accordance with the procedure below: Older KS2 pupils may have a junior e-mail account but staff **must view** all e-mails before transmission, and read incoming mail before the child. Communications with persons and organisations will be managed to ensure appropriate educational use and that the good name of the school is maintained.

Role of pupils:

Internet access will be planned to enrich and extend learning activities as an integrated aspect of the curriculum.
Pupils are expected to follow the guidance for Internet use and tell a teacher immediately if they encounter any material that makes them feel uncomfortable or is inappropriate.
Pupils will use the hot links provided for relevant and suitable websites.
Pupils will be educated in and expected to take personal responsibility when using the Internet.
Pupils will be informed that checks can be made on files held on the system. Pupils may send internal e-mails as part of planned lessons.
We use a wide range of strategies to support children with additional needs who might need extra support to keep themselves safe, especially online.

- Sensitively check pupil's understanding and knowledge of general personal safety issues using reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.
- Apply rules consistently to embed understanding.
- Communicate rules clearly to parents and seek their support in implementing school rules at home. Working with parents and sharing information with them is relevant to all children, but this group especially.
- Careful explanations about why rules might change in different situations
- Consistent use of cause and effect linking the rules to consequences teaching realistic and practical examples of what might happen without frightening pupils.

Role of Parents/Carers:

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. The school will help parents understand internet safety issues through parents' evenings, newsletters, letters, website.

The key responsibilities for parents are to:

- support the school in promoting online safety which includes the pupils' use of the Internet and the school's use of photographic and video images;
- work with and support the school when issues or concerns are identified which are as a result of the school's filtering and monitoring procedures and processes;
- promote acceptable internet use and encourage their child to follow it;
- consult with the school if they have any concerns about their child's and others' use of technology;

- promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology (including on social media) by ensuring that they themselves do not use the Internet/social network sites/other forms of technical communication in an inappropriate or defamatory way;
- support the school's approach to online safety by not uploading or posting to the Internet any images or details of others without permission and refraining from posting pictures, video or text that could upset, offend, or threaten the safety of any member of the school community or bring the school into disrepute.

Sharing nude and/or semi-nude images and/or videos:

Where incidents of the sharing of nude and/or semi-nude images and/or videos via the internet or mobile phone by those under the age of 18 are discovered , we will refer to the UK Council for (UKCIS) guidance 'Sharing nude and semi-nude images'. A copy of this document is available from the school office. Where one of the parties is over the age of 18 and the other is under 18, we will refer to it as child sexual abuse.

All staff and other relevant adults have been informed of how to deal with how to respond to an incident in recognition of the fact that it is generally someone other than the DSL who will first become aware of an incident. Staff, other than the DSL, must not intentionally view, copy, print, share, store or save or delete the image or ask anyone else to do so but must report the incident to the DSL as soon as possible.

It is the responsibility of the DSL to follow the guidance issued by UKCIS, decide on the next steps and whether to involve other agencies as appropriate.

It is important to understand that whilst the sharing of nude and/or semi-nude images and/or videos is illegal, pupils should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue.

The UKCIS advice outlines how to respond to an incident of nudes and semi-nudes being shared including:

- risk assessing situations;
- safeguarding and supporting children and young people;
- handling devices and images;
- recording incidents, including the role of other agencies.
- informing parents and carers

The types of incidents which this advice covers are:

- a person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18;
- a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18;
- a person under the age of 18 is in possession of nudes and semi-nudes created by another person under the age of 18.

Upskirting:

All staff are aware that 'upskirting' (taking a photo of someone under their clothing) is now a criminal offence, but that pupils should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue. If staff or other adults become aware of an incident of 'upskirting', the issue must be reported to the DSL as soon as possible.

Cyberbullying:

Cyberbullying (also known as online bullying) can be defined as the use of information and communications technology particularly mobile devices and the internet, deliberately to upset someone else and reported incidents will be treated in the same way as any other form of bullying. The Behaviour Policy and procedures will be followed in relation to sanctions taken against the perpetrator. It is important not to treat online bullying separately to offline bullying and to recognise that some bullying will have both online and offline elements. Support will be provided to both the victim and the perpetrator. In some cases, it may be necessary to inform or involve the Police.

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming, or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are several statutory obligations on schools in relation to behaviour which establish clear responsibilities to respond to bullying. In particular, section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's Behaviour Policy which must be communicated to all pupils, school staff and parents;
- gives Head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Sexual violence and harassment:

DfE guidance on sexual violence and harassment is referenced in Part five of 'Keeping Children Safe in Education'. All staff are aware of this guidance.

We have a zero tolerance approach to all forms of sexual violence and harassment and will act appropriately on information which suggests inappropriate behaviour regardless of the considered seriousness. Any incident of sexual harassment or violence (online or offline) must be reported to the DSL at the earliest opportunity. The DSL will follow the guidance as outlined in the Child Protection Policy and procedures. Sanctions will be applied in line with our Behaviour Policy and procedures.

Misuse of school technology (devices, systems, networks, or platforms):

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Where pupils contravene these rules, the Behaviour Policy and procedures will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct and, where necessary, the school disciplinary procedures.

The school reserves the right to withdraw, temporarily or permanently, any or all access to such technology or the right to bring mobile technology devices onto school property.

Social media incidents:

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by an identifiable member of the school community, we will request that the post be deleted and will expect this to the actioned promptly.

Where an offending post has been made by a third party or is anonymous, the school may report it to the hosting platform, the Police or may contact the Professionals' Online Safety Helpline (UK Safer Internet Centre) for support or assistance in accelerating the process of removal.

Data protection and data security:

All pupils, staff, Governors, parents, and other adults working in or visiting school are bound by the school's Data Protection Policy and procedures a copy of which is available from the school office.

There are references to the relationship between data protection and safeguarding in key DfE documents i.e. Keeping Children Safe in Education and Data protection: a toolkit for schools which the DPO and DSL will seek to apply.

The Head teacher, DPO and Governors work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always the primary consideration and data protection processes support careful and legal sharing of information. The Data Protection Act 2018 does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with the DPA. Legal and secure information sharing between schools, Children's Social Care and other local agencies is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not** be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

All pupils, staff, Governors, volunteers, contractors, and parents are bound by the school's Data Protection Policy and procedures.

Social Media

Managing social networking, social media, and personal publishing sites:

Online reputation management is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Negative coverage almost always causes some level of disruption and can result in distress to individuals.

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

The school has an official Facebook account which is managed by the school and will respond to general enquiries about the school, but we ask parents not to use these channels to communicate about their children or other personal matters.

Email (via governor, staff, and pupil school email addresses only), Tapestry and Scholar Pack ParentsApp are the official online communication channels between parents and the school, and between staff and pupils.

Staff, pupils', and parents' Social Media presence:

Social media is a fact of modern life and, as a school, we accept that many parents, staff and pupils will use it. However we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

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

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure (available via the school website) should be followed.

We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation, or abuse. However, children will often learn most from the models of behaviour they see and experience. Parents can best support this by talking to their children about the apps, sites, and games they use, with whom, for how long, and when.

Parents and carers are discouraged from 'following' or 'adding' staff, Governors, volunteers, or regular school contractors accounts. However, we accept that this can be difficult to control. This, however, highlights the need for staff to remain professional in their private lives. Conversely staff must not follow pupil accounts.

Staff are reminded that they should not bring the school or profession into disrepute and the best way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. Staff must never discuss the school or its stakeholders on social media and ensure that their personal opinions are not attributed to the school.

Pupil use of personal devices:

- Pupils are not permitted to bring mobile phones or personal electronic devices into school.
- If a pupil breaches the school procedures, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents in accordance with the school Behaviour Policy and procedures.
- If a pupil needs to contact a parent/carer, this will be done via the school telephone. The same applies if parents/carers need to contact their child.

Staff use of personal devices:

- Staff are not permitted to use their own personal phones or devices for contacting children, young people, and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents is required.
- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode; Bluetooth communication should be "hidden" or switched off, location data switched off unless being used only for the duration of a specific task like route directions on a school trip, and mobile phones or personally owned devices will not be used during teaching periods unless permission has been given by the Head Teacher.
- Where members of staff are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then the Head Teacher will give prior permission for this. In an emergency where a staff member does not have this, they should use their own device and hide their own mobile number for confidentiality purposes.
- If a member of staff breaches the school Policy and procedures, then disciplinary action may be taken.

Parents are asked to keep phones out of sights whilst on the school premises. They must ask permission before taking any photos e.g. of displays in corridors or classrooms and avoid capturing other children. If required, urgent messages can be passed onto pupils via the school office.

Managing filtering and monitoring:

Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn we (the Governors, SLT and staff) will do all we reasonably can to limit children's exposure to online safety risks from the school's IT system. As part of this process, we will

ensure that the school has appropriate filtering and monitoring systems in place and will regularly review their effectiveness.

By making use of an appropriate risk assessment, the school will work towards meeting the obligations set out in the DfE filtering and monitoring standards which set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs

The Governors will review the standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting the standards.

The following issues will be addressed and regularly reviewed in relation to the management of filtering:

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with the School's Broadband team to ensure that filtering procedures are continually reviewed.
- The school will have a clear procedure for monitoring and subsequent reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the DSL who will then record the incident and escalate the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the SLT.
- The school SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

Cyber security and resilience:

It is vital that the school understand our vulnerabilities in relation to potential cyber-attacks and breaches, regularly review our existing defences and take the necessary steps to protect our networks. As well as having a current and cohesive Cyber Response Plan in place, there are several measures that we can implement to help to improve our IT security and mitigate the risk of a cyber-attack.

Complaints:

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable materials will never appear on a school computer or mobile device. Neither the school staff nor the Governing Body/Board of Directors can accept liability for material accessed, or any consequences of internet access.

- Complaints about the misuse of on-line systems will be dealt with under the school's Complaints procedure.
- Complaints about cyberbullying are dealt with in accordance with our Anti-bullying procedures which form part of our Behaviour Policy and procedures.

- Complaints related to child protection are dealt with in accordance with school Child Protection Policy and procedures.
- Any complaints about staff misuse will be referred to the Head teacher.
- All online safety complaints and incidents will be recorded by the school including any actions taken.7

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by class teacher/Head of Year/Online Safety Coordinator/Head teacher;
- informing parents;
- removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework);
- referral to the Police.

Monitoring and Review:
The Headteacher will ensure that the policy is implemented effectively.

This policy will be reviewed annually, or sooner if necessary, by the Governing Body and Head Teacher.

REVIEW SHEET – Internet Safety & Access Policy

The information in the table below provides details of the earlier versions of this document and brief details of reviews and, where appropriate, amendments which have been made to later versions.

Version Number	Version Description	Date of Revision
1	Original	May 2018
2	Information added on all sections. New sections and sub-sections added: Social Media, Filtering and Monitoring, Use of personal devices, Misuse of technology, sexual vioence and harassment, upskirting, cyberbullying, sharing of nude images	Sept 2023
3	No changes made at annual review	Sept 2024
