A COMMITTMENT TO EXCELLENCE

Online Safety Policy

Policy & Procedure Number: 69

Date of Board of Governors Review: Autumn 2025

Next Review Due: Autumn 2026

School Link: Nicola Harrison

Revision Number: v01

MEMBER OF THE WADE DEACON TRUST

Contents

1. Introduction

1.1 ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

1.2 Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Learning Platforms and Virtual Learning Environments;
- Generative Artificial Intelligence
- Email and Instant Messaging;
- Chat Rooms and Social Networking;
- Blogs and Wikis;
- Podcasting;
- Video Broadcasting;
- Music Downloading;
- Gaming;
- Mobile / Smart phones with text, video and/ or web functionality;
- Other mobile devices with web functionality.

1.3 Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

1.4 We understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom

2. Aims

2.1 At Wade Deacon High School we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Identify and support groups of pupils that are potentially at greater risk of harm online than others;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones');
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2.2 The 4 key categories of risk;

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes;

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and,
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

3. Legislation, guidance and policy

3.1 This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

3.2 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3.3 The policy also takes into account the National Curriculum computing programmes of study.

3.4 Both this policy and the **Acceptable Use Agreement** (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc…).

3.5 This policy should be read alongside the following policies: Safeguarding & Child Protection Policy, RSHE Policy, Behaviour for Learning Policy, Bullying Policy, Code of Conduct, Safer Working Practices, Mobile Phone Policy.

4. Roles and responsibilities

4.1 The governing body

4.1.1 The governing body has overall responsibility for monitoring this policy and holding the Executive Principal/ Head of School to account for its implementation.

4.1.2 The governing body will ensue all staff at Wade Deacon High School undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

4.1.3 The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff briefings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

4.1.4 The governing body will make sure that Wade Deacon High school teaches pupils how to keep themselves and others safe, including online.

4.1.5 The governing body will make sure that Wade Deacon High school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. They will review the DfE's filtering and monitoring standards, and discuss with the ICT Manager and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet the school's safeguarding needs.

All governors will:

- Make sure they have read and understand this policy;
- Agree and adhere to the terms on the **Acceptable Use Agreement** of the school's ICT systems and the internet (appendix 2);
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures;
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

4.2 The Executive Principal – Mr Brendan Hesketh

4.2.1 The Executive Principal is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Head of School – Mr Matthew Deeney

4.3.1 The Head of School is also responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

4.4 The Designated Safeguarding Lead (DSL) – Mrs Nicola Harrison

4.4.1 The contact details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

4.4.2 The DSL takes lead responsibility for online safety in school and has, along with members of the Safeguarding Team, completed relevant online safety training so they are aware of the potential for child protection / safeguarding issues to arise from students' use of technology. Potential issues may include:

- Sharing of personal data;
- Access to illegal / inappropriate materials;
- Inappropriate on-line contact with adults/strangers;
- Sharing of nudes & semi-nudes;
- Child-on -Child abuse / Sexual Violence & Sexual Harassment;
- Potential or actual incidents of grooming / exploitation;
- Bullying;
- Generative AI
- Terrorism and extremism material.

4.4.3 The DSL's responsibilities include:

- Supporting the Executive Principal/Head of School in making sure that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Executive Principal/Head of School and governing body to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly;
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks;
- Working with the ICT manager to make sure the appropriate systems and processes are in place and provide governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly;
- Working with the Executive Principal /Head of School ICT manager and other members of the safeguarding / Care, Guidance and support team, as necessary, to address any online safety issues or incidents;
- Managing all online safety issues and incidents in line with the school's child protection policy;
- Working with the ICT manager and other members of the safeguarding / Care, Guidance and support team, as necessary, to respond to safeguarding concerns identified by filtering and monitoring;
- Working with the safeguarding and Care, Guidance and Support Team, make sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy;
- Working with the safeguarding and Care, Guidance and Support Team, make sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety;
- Working with the safeguarding and Care, Guidance and Support Team, liaise with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the Executive Principal/Head of School and/or governing body, including child-on-child abuse which may take place online;
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively;

This list is not intended to be exhaustive.

4.4.4 The other members of the Safeguarding Team are;

- Matthew Deeney – Head of School
- Claire Ward – Vice Principal
- Josie Gallagher – Vice Principal
- Adam Mitchell – Senior Assistant Vice Principal
- Kirsty Bryan – Deputy Leader of Care, Guidance and Support
- Claire Rylands – PEP Co-Ordinator
- Abbie Morley – Learning Mentor with family engagement responsibility

4.5 The ICT Network Manager – Ben Watts

4.5.1 The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils

are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;
- This list is not intended to be exhaustive.

4.6 All staff and volunteers

4.6.1 All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2);
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting a concern with "ICT support" via the icon on the desktop;
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes by requesting access to a site via "ICT support" on the desk top;
- Working with the DSL to make sure that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy;
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy and logged on CPOMS;
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'. All concerns of this nature should be discussed face to face with the DSL/safeguarding team and logged on CPOMS;
- This list is not intended to be exhaustive.

4.7 Parents/carers

4.7.1 Parents/carers are expected to:

- Notify a member of staff of any concerns or queries regarding this policy;
- Make sure that their child has read, understood and agreed to the terms on the schools **Acceptable Use Agreement** of the school's ICT systems and internet.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

4.8 Visitors and members of the community

4.8.1 Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it.

4.8.2 This policy, supported by the school's **Acceptable Use Agreement** (for staff, governors, visitors) is to protect the interests and safety of the whole school community).

5 Educating pupils about online safety

5.1 All staff incorporate online safety activities and awareness within their curriculum areas. This is also taught through the school's Personal Development programme as well as through pastoral messages and assemblies. Students sign to say they have read the **Acceptable Use Agreement** (Appendix 2). Parents / Carers are also informed about this. We ask that parents agree to support and uphold the principles of the **Acceptable Use Agreement** in relation to their child's use of the Internet, at home and at school. We also ask parents / carers to uphold the principles of this policy in relation to their own use of the Internet, when the use is related to school, employees of the school and other students at the school.

5.2 It is essential that children are safeguarded from potentially harmful and inappropriate online material. The school has a duty to protect and educate pupils, and staff in their use of technology and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

5.3 At Key Stage 3, online safety is mainly taught through the computing curriculum but also taught through the personal development curriculum in line with Relationships and sex education and health education. In teaching students about online safety, the school uses the DFE's guidance on how to stay safe online: *Teaching online safety in school* (June 2019) which has a focus on the following areas:

- Knowledge and behaviours;
- Harms and risks;
- Navigating the Internet and managing information;
- How to stay safe online;
- Well-being

5.4 In KS3 pupils will also be taught:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in KS4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- How to report a range of concerns;

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them;
- What to do and where to get support to report material or manage issues online;
- The impact of viewing harmful content;
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners;

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail;
- How information and data is generated, collected, shared and used online;
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours;
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online);
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online;

5.5 Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6 Educating parents/carers about online safety

6.1 The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or Synergy. This policy will also be shared with parents/carers.

6.2 Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use;
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

6.3 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Principal/Head of School and/or the DSL.

6.4 Concerns or queries about this policy can be raised with any member of staff or the Executive Principal/Head of School.

7 Preventing and addressing cyber-bullying

7.1 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

7.2 The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

7.3 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal Development and other subjects where appropriate.

7.4 All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. There is also information for parents/carers on the school website, so they are aware of the signs, how to report it and how they can support children who may be affected. Guidance for parents and updates are also sent via school synergy, newsletters and end of term letters.

7.5 In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

7.6 The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.7 To ensure pupils are safe online, the school has an enhanced monitoring and filtering system called Smoothwall. Smoothwall will detect any concerning words which are typed on a school computer linked to specific safeguarding harms, as well as inappropriate or concerning searches, images, uploads or downloads. School systems are monitored 24/7 and 365 days a year by Smoothwall and any concerning or offensive words, searches, images, uploads or downloads (even if deleted immediately) will trigger a response. Smoothwall will contact the Safeguarding Team, either by email or telephone (in case of emergency) and inform the school of the username of the pupil who the concern is related to.

7.8 When the Safeguarding Team receive an alert, a member of the team will speak to the pupil about the information received. Where necessary, parents / carers will be informed and the information logged on CPOMs using the category: Smoothwall. Depending on the information received, appropriate support will be offered. Incidents of inappropriate use will be dealt with in line with other school policies such as: Behaviour for Learning, Safeguarding & Child Protection and Anti-Bullying.

7.9 The purpose of Smoothwall is not to invade a pupil's privacy but to ensure that everyone in school is safeguarded and can receive the right support if and when needed. It is also to ensure that school can effectively deal with potential bullying or abuse and is in line with the school's **Acceptable Use Agreement** which is signed by students.

8 Examining electronic devices

8.1 The Executive Principal/Head of School, and any member of staff authorised to do so by the Executive Principal/Head of School, as set out in the BFL policy can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or;
- Is identified in the school rules as a banned item for which a search can be carried out, and/or;
- Is evidence in relation to an offence.

8.2 Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Executive Principal, Head of School or DSL;
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it;
- Seek the pupil's co-operation.

8.3 Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or;
- Undermine the safe environment of the school or disrupt teaching, and/or;
- Commit an offence;
- If inappropriate material is found on the device, it is up to the Executive Principal, Head of School or DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

8.4 When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or;
- The pupil and/or the parent/carer refuses to delete the material themselves;
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- **Not** view the image;
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

8.5 Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Wade Deacon's Behaviour for Learning Policy.

8.6 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9 Artificial intelligence (AI)

9.1 Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

9.2 Wade Deacon High School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

9.3 Wade Deacon High School will treat any use of AI to bully pupils very seriously, in line with our BFL and Anti Bullying policy.

9.4 Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by Wade Deacon High School and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

10. Acceptable use of the internet in school

10.1 All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

10.2 Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

10.3 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

10.4 More information is set out in the acceptable use agreements in appendices 1 and 2.

11. Prevent

11.1 Under duties imposed within the Prevent Duty Guidance as part of the Counter-Terrorism and Security Act 2015, Wade Deacon High School will ensure that situations are suitably risk assessed, that they will work in partnership with other agencies, that all staff are suitably trained and that IT policies will ensure that children and young people are safe from terrorist and extremist material when accessing the Internet in school.

11.2 The School Lead (Single Point for Contact) for Prevent is: Nicola Harrison. The SPOC will link with other relevant agencies (including the Police) to ensure that vulnerable people are appropriately supported and risk assessed, and that staff and governors are trained to an appropriate level to ensure they are able to recognise any concerns. The specific Roles and Responsibilities of this Single Point of Contact (SPOC) are defined in the school's Child Protection & Safeguarding Policy.

12. Remote Learning

12.1 There may be occasions where the school will need to implement a 'remote learning' approach to education. This might be due to health reasons or when extreme weather prevents the school from fully opening.

12.2 It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection & Safeguarding Policy and where appropriate referrals should still be made to Children's Social Care (iCART) and as required, the police. Contact details can be found in the Safeguarding and Child Protection Policy.

12.3 Online teaching should follow the same principles as set out in the school's Code of Conduct and in line with Guidance for Safer Working Practice. Below are some factors to consider if there are virtual lessons, especially where webcams are involved:

- No 1:1s; groups only unless this has been agreed;
- Staff and children must wear suitable clothing, as should anyone else in the household;
- Any computers used should be in appropriate areas, for example, not in bedrooms and the background should be blurred;
- The live class should be recorded so that if any issues were to arise, the video can be reviewed;
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day;
- Language must be professional and appropriate, including any family members in the background;
- Staff must only use platforms specified by senior managers and approved by our IT

network manager / provider to communicate with pupils;
- Staff should record the length, time, date and attendance of any sessions held.

13. Password Security

13.1 Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are regularly reminded of the need for password security. Staff are required to set their own password that meets the security requirements set out by the ICT team. Staff must regularly change passwords and ensure they are not shared.

13.2 If staff believe their password may have been compromised or someone else has become aware of their password, they must report this to ICT Support.

13.3 Staff are made aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform.

13.4 All users must make sure that workstations are not left unattended and are locked.

13.5 In school, all ICT password policies are the responsibility of the System Manager and all staff are expected to comply with the policies at all times.

14. Data and Security

14.1 The accessing and appropriate use of school data is something that the school takes very seriously. The school follows the Information Commissioners Office (ICO) guidelines:

- Staff are made aware of their responsibility when accessing school data;
- The Level of access is determined by either the Executive Principal/Head of School and / or the ICT Network Manager;
- Confidential or sensitive data taken off the school premises must be encrypted;
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any confidential or sensitive data without the express permissions of the Executive Principal/Head of School;
- Only software properly purchased and / or approved by ICT Support may be used on the school's hardware. It is the responsibility of the user to ensure that ICT Support is fully consulted if they wish to install additional software on their laptop. It is also the responsibility of the user to ensure that any licensing issues are addressed promptly;
- It is policy to store data on a network drive which is backed up each day. It is the responsibility of each individual user to ensure that data not stored on the network is backed up regularly. The School does not take responsibility for data not in the backup plan being lost, deleted stolen etc...;
- Personal devices (Laptops, Mobile Phones etc...) are not permitted to be used on the system, or connected to the wireless infrastructure without the express permissions of the Executive Principal/Head of School and / or ICT Network Manager;
- The school does not guarantee the security of any information users may enter while making permitted personal use of a school computer. The school disclaims all liability that may arise from loss or harm suffered by a user as a result of that information being disclosed to or obtained by any other person and then being further disclosed or being used so as to cause loss to the user. The school disclaims all liability for such losses and any employee using a school computer for permitted private purposes does so on the basis of having agreed this disclaimer of liability;
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the system manager's to install or maintain virus protection on personal systems;
- If there are any issues related to viruses or anti-virus software, the ICT Network Manager should be informed.

15. Managing the Internet

15.1 The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected, it will be followed up.

15.2 All users must observe software copyright at all times. It is illegal to copy or distribute school software, non-licensed software or illegal software. All users must observe copyright of materials from electronic resources.

15.3 Staff will preview any recommended sites before use. Raw image searches are discouraged when working with pupils. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents / carers recheck these sites and supervise this work. Parents / carers will be advised to supervise any further research.

16. Infrastructure

16.1 School Internet access is controlled through the NetSweeper web filtering software with a bought in whitelist solution.

16.2 Wade Deacon High School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018/GDPR, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

16.3 The school ensures children are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering in accordance with the Prevent Duty Guidance.

16.4 Staff are aware that school Internet activity can be monitored and explored further if required. Intrusions into the privacy of employees must be proportionate to the purpose of the monitoring.

16.5 The school uses SMART Sync management control tools for controlling and monitoring workstations. If staff discover an unsuitable site, the incident must be reported immediately to the System manager or the Safeguarding Team.

16.6 It is the responsibility of the school, by delegation to the ICT Network Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

16.7 Staff are not permitted to download programs on school-based technologies without seeking prior permission from ICT Support.

17. Managing email

17.1 The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

17.2 The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep

their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. This should be the account that is used for all school business. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

17.3 Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending emails to external organisations, parents / carers or pupils are advised to cc. their Line Manager. The forwarding of chain emails is not permitted in school. All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication. Pupils' initials are recommended to be used in correspondence rather than the full name.

17.4 Staff must inform either their line manager or System Manager if they receive an offensive email.

17.5 The School will assist the relevant authorities in taking action against any employee who commits an unlawful act whilst using the School's computer facilities. The School will report criminal activity to the Police.

17.6 Personal or business emails, whether created or stored on School equipment, constitute a School record and as such are deemed to be property of the School.

17.7 Emails from unknown sources or which may appear suspicious must not be opened. Software received via email must not be installed. You must consult ICT Support for advice if you receive software via email or email from an unknown source or which is otherwise suspicious.

17.8 Emails are formal documents and must not contain remarks that might be potentially embarrassing to the School, its employees or the general public.

18. Managing other Web 2 technologies

18.1 Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

18.2 At present, the school allows access to social networking sites for staff within school; this allows for better connectivity with a range of online learning technologies.

18.3 School staff with social networking profiles should ensure that they set the privacy levels on their accounts to the maximum i.e. only people on their 'friends or trusted' lists should be able to view their pictures / private information.

18.4 The school specifies the following guidelines should a message from a student be received:

- Do not reply to the message. Replying to a message allows the recipient to view your profile in its entirety. This is also a way to circumvent the privacy settings on accounts;
- Inform the school's Safeguarding Lead at the earliest opportunity and advise them of the full details of the incident. The relevant communication should be made available to the member of staff to aid in any investigation.

18.5 The School advises staff to keep their account privacy as high as possible. Any contact from a pupil, or attempted contact, must be immediately reported to the school Safeguarding Lead. Staff should not respond to any contact / request for contact from any pupil other than to delete / block.

18.6 As a professional, you must remember that in addition to protecting yourself, you should not participate in anything via social media that would bring your employer into disrepute.

18.7 All staff are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

18.8 Staff are encouraged to be wary about publishing specific and detailed private thoughts online. A general rule is don't post/share/tweet/re-tweet anything you would not be happy for your Executive Principal to see.

19. Mobile technologies

19.1 Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and then risk assessed before use in school is allowed.

20. Personal Mobile devices (including phones)

20.1 The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device.

20.2 Staff are advised to always contact parents / carers using the school's phone system. If a member of staff does need to contact a parent / carer using their own device, they should do so via the 3CX app on their mobile phone. This enables all calls to go through the school's phone system. If this is not possible, personal numbers from devices should be blocked.

20.3 The school is not responsible for the loss, damage or theft of any personal mobile device.

20.4 The sending of inappropriate text messages between any members of the school community is not allowed.

20.5 Whilst on the premises or while conducting official school business, permission must be sought before any image or sound recordings are made on personal devices by any member of the school community.

20.6 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

20.7 While in school, personal mobile phones shall be set on discreet mode.

20.8 Mobile phones shall only be used in work in accordance with instructions issued by the school's mobile phone guidelines.

21. School provided devices (including phones)

21.1 Where the school provides mobile technologies such as phones or laptops for offsite visits and trips, only these devices should be used to conduct school business.

21.2 Fixed telephony equipment must not be moved, unplugged or switched off except with the express permission of ICT Support.

21.3 Settings on telephones must not be altered as this could cause a failure to ring. Proper use of divert or follow me facilities is permitted.

21.4 Personal incoming calls (by landline or mobile) or faxes with the exception of emergencies whilst at work, should be discouraged and where unavoidable must be kept to a minimum.

22. Taking of Images and Film

22.1 Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

22.2 With the written consent of parents / carers (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

22.3 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils; this includes when on field trips. However, with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

23. Publishing pupils' images and work

23.1 On a child's entry to the school, all parents / carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website;
- On the school's Twitter / Instagram pages / Social Media pages;
- In the school prospectus and other printed publications that the school may produce for promotional purposes;
- Recorded / transmitted on a video or webcam;
- In display material that may be used in the school's communal areas;
- In display material that may be used in external areas, i.e. exhibition promoting the school;
- General media appearances, e.g. local / national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

23.2 This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

23.3 Parents / carers may withdraw permission, in writing, at any time. Consent has to be given by both parents / carers in order for it to be deemed valid.

23.4 Students' full names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published.

23.5 Before posting student work or images external to the school, e.g. on the Internet or distributing to the Press, a check needs to be made to ensure that permission (from the parents / carers and the pupil) has been given for work to be displayed. This is the responsibility of the member of staff submitting the information.

24. Storage of Images

24.1 Images / films of children are stored only on the school's network. Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Executive Principal/ Head of School. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network / Learning Platform. Images must be deleted when they are no longer required.

25. Webcams and CCTV

25.1 The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.

25.2 We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes. Consent is sought from parents / carers and staff on joining the school, in the same way as for all images.

26. Complaints

26.1 Complaints relating to online safety should be made to the Principal. All incidents should be logged.

27. Inappropriate material

27.1 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Network Manager.

27.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Network Manager.

Appendix 1 - Staff Acceptable Use Agreement

This is the Acceptable Use Agreement for our school. The purpose of this policy is to promote positive and responsible network and Internet behaviour. Please read carefully; by acknowledging that you have read this policy, you will be indicating that you agree to the terms set out below.

Staff:

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of SLT.
- I will not divulge any school related passwords and I will comply with school IT security procedures.
- I will make sure email with staff, parents, pupils and members of the public are responsible and in line with school policies.
- I will not give my home address, phone number, mobile number, personal social networking details or personal email address to pupils.
- I accept that pupils may find these details out, and that any contact should be logged and either not reciprocated, or replied to in line with school policies. I should be responsible and aware of my professional responsibilities and school policies if I supply any personal details to parents.
- I will use school email systems for school related communications. I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Act / GDPR. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment.
- I will not install software onto workstations or the network unless supervised by the Network Manager or IT support staff.
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory or copyright infringing using school IT equipment.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent / guardian. I will ask the permission of the Principal (on site) or the proprietor of the building (off site) prior to taking any photographs.
- I am aware that all network and Internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute.
- I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with school policy.
- I will champion the school's e-safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will not make comments about school on personal social media, whether positive or negative.
- I will not use my personal phone or camera to take photographs of pupils even if this is for a school purpose.

Appendix 2 - Acceptable Use Agreement for pupils 2025-2026

This is the acceptable usage policy for our school. The purpose of this policy is to promote positive and responsible network and Internet behaviour. Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the school's IT systems.

Pupils:

- I will only use school Internet and IT facilities for educational purposes which follow the teachers' instructions. This includes email, video, messaging, video-conferencing, social media, Internet, file-saving and printing.
- I will only use my mobile phone or mobile device in school when permission has been granted by a teacher. If permission is granted, I will use my mobile device as if it was a school computer, following all the rules for using school computers.
- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses. I will ask an ICT teacher to install software if required.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to.
- I will only use my school-supplied email address for school-related activities.
- I will not look at or delete other people's work or files.
- I will make sure all my contact with other people at school is responsible. I will not cyber-bully pupils or teachers.
- I will be responsible and polite when I talk online to pupils, teachers and other people related to the school, both in school-time and outside school-time.
- I won't look for or look at unpleasant or inappropriate websites in school. I will check with a teacher if I think a website might be unsuitable.
- I won't give out my personal details, such as my name, address, school or phone number on the Internet.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I won't upload or download any pictures, writing or films which might upset people online.
- I won't write unpleasant, rude or untrue comments online about pupils, teachers or the school.
- I will treat all IT equipment at school with respect and ensure the computer is left in the state that I found it.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a teacher is concerned about my online safety or my behaviour when using school computers.
- I will respect copyright when making use of images and videos in my school work.
- I will not look for, view, upload or download offensive, extremist, illegal, copyright-infringing or pornographic material. If I find such material on school IT equipment I will inform a teacher immediately.
- Images of pupils will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet or in the media with permission.
- I am aware that the school uses an online monitoring and filtering system called Smoothwall to safeguard students.
- I am aware that Smoothwall will alert school if any concerning or offensive words, searches, images, uploads or downloads (even if deleted immediately) are accessed on school systems.
- I am aware that school will use the Smoothwall system to offer appropriate support but also to ensure that it can effectively deal with potential bullying or abuse. Such instances may be dealt with in line with the school's Behaviour for Learning Policy and the Anti-Bullying Policy.
- I will not look for ways to bypass the school filtering or proxy service or bypass the school filtering or proxy service.
- I understand that these rules are designed to keep me safe and that if they are not followed, sanctions may be applied and my parent/guardian may be contacted.

Full name: Form group:

Signed: Date: