Online Safety Policy

WATERGATE SCHOOL

'I Can, You Can, Together We Will'

Written by: Linda Matthews

Updated: October 2024

Next Review: October 2027

INTRODUCTION

At Watergate School we feel that it is important to adhere to a strict online safety policy to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any concerns where appropriate.

Online safety is a safeguarding issue and overall responsibility for online safety is held by the designated safeguarding lead and deputy designated safeguarding leads. The named online safety co-ordinator is Simon Wright.

Online safety can be categorised into three broad areas of risk that cover a wide range of potential issued related to online safety:

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

RATIONALE

Technology is an integral part of the school's curriculum and offers evolving opportunities. Access to online resources is becoming universal and more mobile, with pupils accessing technology at an early age.

AIMS

1. To ensure that all pupils can access ICT devices at school safely.
2. To ensure that all personal data is secure on the school network.
3. To provide guidance to adults regarding the appropriateness of material that they access at school.
4. To share information with parents on appropriate use of ICT devices at home.

TECHNICAL AND INFRASTRUCTURE APPROACHES

Watergate School:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of anti-virus software etc and network set-up so staff and pupils cannot download executable files;
- Uses individual log-ins for all adults.
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;

- Provides staff with an email account for their professional use, using Office365and makes clear personal email should be through a separate account;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Uses the software 'Classroom Cloud' to monitor the use of curriculum devices (computers and iPads. The school does all that we reasonably can to limit children's exposure to risks from the school's IT system. The leadership team and relevant staff should have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns identified. When making filtering and monitoring decisions, the school will consider those who are 'potentially at greater risk of harm' and how often they access the IT system along with the proportionality of costs versus safeguarding risks.
- Regular risk assesses the school's online safety systems in co-ordination with technical support to ensure a consistent cycle of monitoring.

POLICY AND PROCEDURES

Watergate School:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common sense strategies in learning areas where older pupils have more flexible access;
- Ensures all staff have signed the staff code of conduct which include acceptable use agreement and that they understand that they must report any concerns;
- Staff will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body. Staff will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business and will not disclose their personal telephone numbers and email addresses to pupils or parents/carers. Staff will not use personal cameras (digital or otherwise) or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home or information related to staff and pupils on personal equipment.
- Informs staff that that they must report any failure of the filtering systems directly to the ICT coordinator. Our ICT coordinator logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the designated safeguarding lead has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides online safety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Should serious online safety incidents occur, the Headteacher will fully investigate, which could lead to disciplinary procedures. See Disciplinary Procedure.

SOCIAL MEDIA- SCHOOL

The school currently runs one social media channel on X. This is managed by a named member of staff who will adhere to the following;

- Only children who have permission for their image to be shared on X will be included on posts
- Names of children will not be used in any posts
- The school will use social media to engage a wide range of interested parties (professionals, parents/carers, families, wider networks etc) and these interactions will remain professional at all times.
- If the named staff running these accounts are concerned by any content the school receives or is tagged in, these will be reported to the Headteacher.
- Security and privacy settings on both accounts are reviewed and on the event of named staff leaving, passwords and permissions will be updated.

SOCIAL MEDIA – PERSONAL

Watergate staff should ensure that, when using social media for personal use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to Watergate School or the local authority

EDUCATION AND TRAINING

Staff:

- Once a year all staff members are refreshed on the online safety policy, especially new additions and all new staff are required to sign an online safety agreement.
- Staff are encouraged to contribute to the policy, and also report any online safety issues to the named online safety coordinator (Simon Wright). These incidents are recorded in the online safety recording document.

Parents:

- Parents are invited to attend an online safety information session. The purpose of this session is to brief them on safe practice with their children. This takes place once a year.

Children:

- Children with appropriate understanding are given input on safe internet and computer practice as part of curriculum learning.

Watergate School

- Fosters a 'No Blame' environment that encourages pupils who are able to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils who are able and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils who are able know how to report any abuse;
- Ensures that staff and pupils who are able understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Provides advice and guidance to parents on an individual basis in the form of leaflets or in school newsletters.

Please also refer to other policies:

- Code of Conduct
- Safeguarding Policy

Acceptable Use Policy (AUP):

Adults working with children agreement form

This covers use of digital technologies in Watergate school: including email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use Watergate school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Management.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system for any email communication related to work at Watergate school.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using Watergate's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of young people or staff without permission and will not store images and documents at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role. I understand that it is my responsibility to ensure I know how to use any such tools so as not to compromise my professional role, such as setting appropriate security settings.
- I agree and accept that any computer or laptop loaned to me by Watergate school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access Watergate school resources remotely (such as from home) only through approved methods and follow online security protocols to access and interact with those materials.
- I understand that it is my duty to support a whole organisation safeguarding approach and I will alert the Watergate school's Designated Safeguarding Lead (Headteacher) or members of the senior leadership team that are Deputy Designated Safeguarding Leads, I feel the behaviour of any service user or member of staff may be a cause for concern or inappropriate.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): 'Staff' agreement form

User Signature

- ☐ I agree to abide by all the points above.
- ☐ I understand that it is my responsibility to ensure that I remain up-to-date and read and understand Watergate school's most recent online safety policies.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....