b

Bramham and Shadwell Federation

‘EXCELLENCE FOR ALL’

Online Safety & Acceptable Use Policy (AUP)

School Policy

Adopted by the: Full Governing Body, September 2021
Updated May 2022
Date to be reviewed: September 2022

Signed:_____
Head teacher

Introduction

At the Bramham and Shadwell Federation, we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This Federation provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The scope of the Code covers fixed and mobile Internet; school PCs, laptops, and digital video equipment. The Computing Leader will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

The Federation is committed to following the Guide to Safer Working Practice (February 2022.) Therefore, our online safety and acceptable use procedures are amended as necessary and we work to ensure that all staff involved in the use of IT to contact pupils and virtual teaching are briefed on best practice and any changes. Senior Leaders are responsible for oversight of this and may join online lessons. Senior Leaders should satisfy themselves that the platform selected for online or virtual teaching has an appropriate level of security; whenever possible staff should use school devices and contact pupils only via the pupil school email address/login. This ensures that the setting's filtering and monitoring software is enables. When making decisions around virtual and online learning, Senior Leaders must take into account a wide range of issues (as stated in GSWP Point 25) and must communicated clear expectations to staff and children.

Individual's responsibilities

Access to the School IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the School IT systems.

Individuals must:

- Not allow anyone else to use their user ID and password on any School IT system.
- Lock their computer when logged into user accounts when left unattended.
- Not use someone else's user ID and password to access School IT systems.
- Protect their passwords by not leaving them unattended e.g. not left on a post it note.
- Not perform any unauthorised changes to School IT systems or information.
- Not attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.

Code of Practice for pupils when in school:

Pupil access to the Internet is through a filtered service provided by Primary ICT, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

In addition, the following key measures have been adopted by The Federation to ensure our pupils do not access any inappropriate material:

- The school's Code of Practice for use of the Internet and other digital technologies is made explicit to all pupils in the form of our School Council Online Safety Tips which is displayed prominently;
- Our Code of Practice is reviewed each school year and shared with pupils;
- Pupils using the Internet will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised, where possible;
- Pupils will, where possible, use areas pre-selected by the teacher and appropriate to their age group;
- Pupils in Key Stage 2 are educated in the safe and effective use of the Internet.
- It should be accepted, that however rigorous these measures may be, they can never be 100% effective. Neither the Federation nor Primary ICT can accept liability under such circumstances.
- The use of mobile phones by pupils is not permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff.
- Pupils who are given special permission to have a mobile phone in school must hand their phone into the school office at the beginning of the day and collect it at the end of the school day. Pupil mobile devices must not be kept in bags, lockers or classroom cupboards.
- During school hours pupils are forbidden to play computer games or access social networking sites, unless specifically assigned by the teacher.

Code of Practice for pupils when working remotely:

- Where students are using digital technology away from school for the purposes of remote learning, the duty to ensure appropriate supervision is the responsibility of the child's parent/carer.
- No recording either by video or photographs should be undertaken by pupils/parents of the live sessions
- Pupils should behave as they would in the "real" classroom and follow school rules and expectations
- Pupils should be on time for lessons and be ready to learn, with equipment and books as directed by their teacher
- Pupils should dress appropriately for lessons, either in school uniform or a similar outfit. Nightwear should not be worn.
- Pupils should sit in a communal area. They should (ideally) not sit in a bedroom and should sit at a desk/table
- Pupils should not use the Teams Chat facility.
- Invitations to live sessions should not be shared with others

Sanctions for pupils in school:

Incidents of technology misuse which arise will be dealt with in accordance with the school's Behaviour Policy. Minor incidents will be dealt with by the Computing Leader in conjunction with the class teacher and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with school child protection procedures.

Sanctions for pupils when working remotely:
If a pupil does not adhere to the code of practice then the Teams call may have to be closed. The teacher will contact the pupil and his/her parents to address the matter. If there is an on-going issue then Senior Leaders will intervene.

Code of Practice for staff in school:

"Creating a culture in which all concerns about adults) including allegations that do not meet the harms threshold – see KCSIE) are shared responsibly and with the right person, recorded and dealt with appropriately, is critical. If implemented correctly, this should encourage an open and transparent culture; enable schools and colleges to identify concerning, problematic or inappropriate behavior early; and minimize the risk of abuse. A culture of vigilance will help to ensure that adults working in or on behalf of the school or college are clear about professional boundaries and act within these boundaries, and in accordance with the ethos and values of the institution."

GSWP February 2022

- Staff should work, and be seen to work, in an open and transparent way including self-reporting if their conduct or behavior falls short of the guiding principles in GSWP

Staff have agreed to the following Code of Safe Practice:

- Pupils accessing the Internet should be supervised by an adult at all times.
- All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed and are discussed with pupils.
- Any website used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate.
- Deliberate/ accidental access to inappropriate materials or any other breach of the school Code of Practice should be reported immediately to the Computing Leader.
- In the interests of system security, staff passwords should only be shared with the Network Manager.
- Teachers are aware that Primary ICT track all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these.
- Photographs of pupils **must always be** taken with a school camera or ipad and images should be stored on a centralised area on the school network, accessible only to teaching staff. These images **must not** be held on personal cameras, phones or laptops.
- School systems may not be used for unauthorised commercial transactions.
- Staff should ensure that they do not allow parents or children to access their email address in the interest of personal safety (see below for the procedure to follow in this instance).

- Staff should be aware of these procedures around the sharing of names and images which are in accordance with our Image Consent Policy:
  In school displays, books a child's image and first name may be shared
  In school publications, an image OR a name may be shared with parental permission
  On the website or in social media, NO names may be shared. Images may be shared with parental permission
- Images will only be shared when photo permissions from parents have been given.
- Staff may have personal mobile phones with them in school when they are needed to fulfil health and safety requirements. This includes the current coronavirus pandemic when school is operating under a specific Risk Assessment. Personal mobiles are to be used when a member of staff requires assistance. They will remain in the staff member's bag/drawer unless required for an emergency and will be used only to make phone calls, which will be done openly, in view of all the class.

Code of Practice for staff:
Staff must follow the Guide to Safer Working Practice; all staff must ensure that they work in accordance with these documents.

Particular reference should be made to the following points:

Point 5:

Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to a senior manager. This is as relevant in the online world as it is in the classroom; staff engaging with pupils and / or parents online have a responsibility to model safe practice at all times.

Point 19

SLT have approved one to one teaching for specific activities such as reading and Talk Times. Parental permission must be obtained before these sessions take place and the GSWP advises that staff should work one to one with a child only when absolutely necessary (both in person or online) and with the knowledge and consent of senior leaders and parents/carers. Staff should be aware of relevant risk assessments, policies and procedures, including child protection, acceptable use policy and behavior management.
"Where staff are expected to work one to one with a pupil on a virtual platform, clear expectations should be set out for all of those involved that are reflective of the settings safeguarding policies and procedures."

Points 8 and 25

Staff should ensure they are dressed decently, safely and appropriately for the tasks they undertake; this also applies to online or virtual teaching.

Advice is also given around background and appropriate areas of a home; filter settings in homes and the age appropriate ratings of resources and videos.

Point 25

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. This includes instances where pupils have not adhered to expectations set by the Federation Code of Practice for pupils.

Staff must be mindful of safeguarding issues within one to one sessions and should report any concerns immediately to the DSL or a Deputy DSL. Point 30 also gives guidance about the duty to report, including self-reporting, any incident in which an adult has or may have behaved in a way that is inconsistent with the organisation's staff code of conduct including inappropriate behaviours inside, outside of work or online.

Staff should recognize their individual responsibility to raise any concerns regarding behavior or conduct (including low level concerns) that falls short of the principles outlined in GSWP and the Federation expectations of staff. It is crucial that any such concerns, including those who do not mean the harm threshold (see KCSIE) are shared responsibly and with the right person, and recorded and dealt with appropriately. Failure to report or respond to such concerns would constitute a failure in professional responsibilities to safeguard children and promote welfare. The GSWP includes guidance around allegations against staff and volunteers, the whistleblowing policy and other reporting channels, including the NSPCC.

Point 25 gives guidance around the recording of lessons which the Federation will consider carefully when the need arises.

If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a member of SLT and if there is no alternative, use caller withheld.

Point 29 gives guidance around student led projects and the safeguarding considerations that should be made.

Internet Safety Awareness

At The Federation we believe that, alongside having this written Acceptable Use Policy which contains our Code of Practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Internet Safety Awareness for Pupils

Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed. In addition, all pupils follow a structured programme of Internet Safety Awareness using a range of online resources.

Internet Safety Awareness for Staff

The Computing Leader keeps informed and updated on issues relating to Internet Safety and attends regular courses. This training is then disseminated to all teaching and support staff on a regular basis.

Internet Safety Awareness for Parents
The School Council Online Safety Tips for children is on our school website.

Prevent

This Policy should be read in conjunction with our Child Protection and Safeguarding Policy and with particular regard to the Prevent Duty. Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". All staff are trained to be aware of the danger of radicalization and the use of the internet to promote values which are not aligned with those of our Federation. Staff are trained to report any concerns around Prevent to the DSL's who follow process as outlined in our Child Protection and Safeguarding Policy.

Health and Safety

The Federation has attempted, as so far as possible, to ensure a safe working environment for pupils and teachers using computing resources, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used.

Personal Safety

Parents and children should only have access the school's main email address and to class email addresses in the event of remote learning.

Teachers and support staff should not allow either children or parents to use their school or personal email address. If a parent or child does access such information, the member of staff should print out any correspondence from the individual(s) and give a copy to Mrs Hilton. Staff should not respond to any correspondence.

Digital and Video Images of Pupils

Parental permission is sought to cover the use of images of pupils on the school website/ TV, Teams calls during remote learning, in the local press, for displays within school. Written permission must be obtained from the parent/ carer for these images to be used.

This ensures that we are following the GSWP guidance (24a) which states that schools should only record a lesson or online meeting with a pupil where this has been agreed with the head teacher or other senior staff, and the parent/carer has given explicit written consent to do so.
Recordings may be made for the use of parents and children who cannot attend live lessons. They are not made using personal equipment and are not for personal use.

School Website (please see Image Consent Policy)

Our school website promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Parental permission is acquired before any images are shared.
- Group photos are used where possible, with general labels/captions.
- Names and images are kept separate – if a pupil is named their photograph is not used and vice-versa.
- Only pupil's first names may be used. Full names should never be shared.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

Storage of Images

Digital and video images of pupils are taken with school equipment. Images are stored on a centralised area on the school network, accessible only to teaching staff. Live Teams lessons will be recorded and stored in the class feed for 20 days. They are only accessible to members of the class team. Recorded lessons will not be published or available to anybody else outside of the class and explicit permission sought from each parent for recording permission.

Social Software

Chat rooms, blogs and other social networking sites are blocked by the Primary ICT filters so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Instances of online bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's Discipline Policy and child protection procedures. Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

Updated May 2022