Online Safety Policy

This Policy applies to the entire setting including the EYFS.

Staff Responsible for policy review: Headteacher, Deputy Head

Next Review: April 2022

Last Review	**Updates made**
April 2021	Renamed E Safety Policy to Online Safety Policy as guidelines dictate.

1. E-SAFETY: POLICY GUIDANCE

1. Scope

This guidance is applicable to all those involved in the provision of e-based education/resources at the school and those with access to / are users of school ICT systems.

2. Objectives

1. To ensure that pupils are appropriately supervised during school activities.
2. To promote responsible behaviour with regard to e-based activities.
3. To take account of legislative guidance, in particular the General Data Protection Regulations and the Data Protection Act 2018.

3. Guidance

1. The School Business Manager / Head Teacher will be responsible for the implementation of this policy.
2. The School Business Manager will act as E- Safety Co-ordinator and will:
   a. compile logs of e-safety incidents;
   b. report to the Head Teacher on recorded incidents;
   c. ensure that staff are aware of this guidance;
   d. provide / arrange for staff training;
   e. liaise with school technical staff;
   f. liaise with the Head Teacher on any investigation and action in relation to e-incidents; and
   g. advise on e-safety policy review and development.
3. The Group IT Manager will:
   a. be responsible for the IT infrastructure and ensure that it is not open to misuse or malicious attack;
   b. ensure that users may only access the networks and devices through an enforced password protection policy;
   c. keep up to date with e-safety technical information in order to carry out their role;
   d. ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse where deemed necessary; and
   e. implement any agreed monitoring software / systems.
4. Teaching and Support Staff will:
   a. maintain awareness of school e-safety policies and practices;
   b. report any suspected misuse or problem to the Head Teacher or E-Safety Co-ordinator;
   c. ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems;
   d. where relevant e-safety is recognised in teaching activities and curriculum delivery;
   e. ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
   f. monitor the use of digital technologies (including mobile devices, cameras etc during school activities); and
   g. ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
5. Child Protection
   a. Those responsible should be trained in e-safety issues and aware of the implications that may arise from:
      i. sharing of personal data;
      ii. access to illegal / inappropriate materials;
      iii. inappropriate contact on-line with adults / strangers;
      iv. potential or actual incidents of grooming; and
      v. cyber-bullying.
6. Pupils
   a. are responsible for using school digital technology systems in accordance with the Group acceptable use policy;

b. will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;

c. will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

d. are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and

e. will understand that the e-safety policy will include actions outside of school where related to school activities.

7. Parents / Carers

a. will be advised of e-safety policies through parents' evenings, newsletters, letters, school website etc;

b. will be encouraged to support the school in the promotion of good e-safety practice; and

c. should follow school guidelines on:

i. digital and video images taken at school events;

ii. access to parents' sections of the school website / pupil records; and

iii. their children's / pupils' personal devices in the school (where this is permitted).

8. Community Users / Contractors

a. Where such groups have access to school networks / devices, they will be expected to provide signed acceptance to abide by school e-safety policies and procedures.

Legal Requirements & Education Standards

References:

A: Commentary on the Regulatory Requirements September 2018, Part 3 (www.isi.net)
B: Reference Guide to the key standards in each type of social care service inspected by Ofsted (www.ofsted.gov.uk)
C: Health and Safety at Work" Section H of the ISBA Model Staff Handbook
D: "Health and Safety and Welfare at Work" Chapter N of the ISBA Bursar's Guide
E: "Insurance" Chapter K of the Bursar's Guide by HSBC Insurance Brokers Ltd
F: UK Council for Child Internet Safety (www.edcuation.gov.uk/ukccis)
G: Cyber-bullying.org (www.cyberbullying.org)
H: Department for Education "Safer Working Practice for Adults who Work with Children and Young People" (www.education.gov.uk)
I: DfE Data Protection: a toolkit for schools

.

Recommended review period: Annual

Review by: Group IT Manager

Date reviewed: February 2020

IT Acceptable Use Policy

Scope of this Policy

This policy applies to all members of the Group community (staff or pupils) who use school IT systems, as a condition of access, and conforms to the statutory safeguarding regulations for online safety laid out in Annex C to Keeping Children Safe in Education 2020. Access to school systems is not intended to confer any status of employment on any contractors.

Online behaviour

As a member of the Group community you should follow these principles in all of your online activities:

- The Group cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the Group community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the Group community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the Group's IT systems

Whenever you use the Group's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the Group's IT systems (this includes non-authorised VPNs and VPN apps), and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the Group's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the Group monitors use of The Group's IT systems, and that the Group can view content accessed or sent via its systems.

Page Break

Passwords

Passwords protect the Group’s network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name, pet’s names or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else’s computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the Group should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Helpdesk.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the Group's right to monitor and access web history and email use.

Use of email

It should be remembered that email can be seen as a formal communication tool. Staff and pupils should afford emails the same etiquette as if they were writing a letter – salutation and signoff should be seen as mandatory.

Use of personal devices or accounts and working remotely

All official school business of staff must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the IT Department.

Where permission is given for use of personal devices (for instance for occasional working from home), these must be subject to appropriate safeguards in line with the Group's policies. You must ensure that your equipment has appropriate passwords enabled, that only you can access your account and that you log out of any sessions once finished.

Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the Group where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The Group may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

Page Break

Compliance with related school policies

To the extent they are applicable to you, you will ensure that you comply with the Group's e-Safety Policy.

Retention of digital data

Staff and pupils must be aware that email accounts will generally be closed and the contents deleted within 3 months of that person leaving the Group. Personal data that is stored within PASS or SharePoint may be kept for 7 years in accordance with DfE requirements.

Any information from email folders that is necessary for the Group to keep for longer, including personal information (e.g. for a reason set out in the Group privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the Group's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Group IT Manager.

Breach reporting

The law requires the Group to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the Group regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the Group's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The Group must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the Group must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, they must email dataprotection@wishford.co.uk with the details, and follow this up with a telephone call either to the Data Protection Officer or the IT Helpdesk to ensure their email has been seen.

Data breaches will happen to all organisations, but the Group must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The Group's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy by staff or pupils will be dealt with as a disciplinary matter using the Group's usual applicable procedures. In addition, a deliberate breach by any person may result in the Group restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the Group community is being harassed or harmed online you should report it to your line manager, or the Compliance Officer. Reports will be treated in confidence wherever possible.

Page Break

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to either your School Business Manager, or the Group IT Manager for head office staff.

I understand and accept this acceptable use policy (staff / pupils):

Name: …………………………………………………………

Signature:

Date:

For younger pupils (below secondary school age)

Name of parent/guardian:

Signature:

Date: