B4L INFORMATION SHARING PROTOCOLS

Weston Point College

Contents

1. General Philosophy....2
2. Expectations for Data Sharing....3
3. External Information Sharing to Parents and Multi-agency Partners....3
4. Internal Reporting for Safeguarding....3
5. External Reporting for Safeguarding.....3
6. Disclosing Personal Data within College....4
7. Disclosing Personal Data outside of College....4
8. Checklist for Data Sharing....4
9. Sharing other Media....4
10. Review Date....4

1. General Philosophy

The Weston Point College Information Sharing Protocol aims to provide clear direction to staff and others about expected codes of behaviour in the sharing of information of a confidential nature.

The protocol also aims to make explicit the organisations commitment to the development of good practice and sound procedures to keep Young People and adults safe.

Information sharing is vital to safeguarding and promoting the welfare of Young People. A key factor identified in many serious case reviews (SCR's) has been a failure by practitioners to record information, to share it, to understand its significance and then take appropriate action. This protocol aims to set out clear standards required by everyone.

Weston Point College follows the Government golden rules of information sharing and these are embedded into everyday practice:

- *Remember that the GDPR is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.*

- *Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.*

- *Seek advice if you are in any doubt, without disclosing the identity of the person where possible.*

- *Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.*

- *Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.*

- *Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.*

- *Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.*

- *Legislation guidelines*

2. Expectations for Data Sharing

All staff should be fully aware of the organisations expectations when sharing information about Young People, adults and their families. Any information that is shared could be requested by the individual or another agency in the future.

Therefore, the information needs to be accurate, factual and does not include personal interpretation or recommendation. Any recordings that are made that are not part of the central, secure recording process must not identify an individual Young Person, adult or their family. In these circumstances the use of initials would be appropriate.

3. External Information Sharing to Parents and Multi-agency Partners

The same principles of sharing information internally, will apply to those members of staff who due to their role and responsibility have permission to share information with parents and multi-agency partners.

Information that is shared externally either electronically or in paper format needs to be sent in a secure method. For example: information that is restricted should be sent password protected (electronically) or via secure email or if sent in paper format, recorded delivery, so that it can be tracked and accounted for.

Information Sharing is necessary in the safeguarding and protection of Young People and all staff within college must follow the Policies where there is any evidence that a child is at risk of significant harm, through observation or disclosure from the child.

4. Internal Reporting for Safeguarding

At any point, if staff believe, in their professional opinion a Young Person is at risk of significant Harm, they must inform the Designated Safeguarding Lead (s) immediately and follow the recording and reporting procedures laid out in our Safeguarding Policy.

Information sharing is also necessary where there are concerns around the behaviour or practice of adults within the setting either employed staff, contractors or visitors. If there are any issues raised about the conduct of any adult on site either towards a Young Person or another adult this must be reported directly to the Head Teacher.

5. External Reporting for Safeguarding.

The role of the DSL is to make a decision based on the information shared about the risk of harm to the Young Person. If the child is deemed to be at risk of significant harm from a person who has care, custody, or control of them then an external referral will be made to the relevant team in the Local Authority (see Safeguarding Policy).
The DSL may also wish to involve the police if the concern is of a criminal nature.

6. Disclosing Personal Data within College

Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the College or their relationship to the data subject, unless they need to know it for a legitimate purpose.

Examples include - personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, pupils or other members of staff unless the member of staff has given their permission.

7. Disclosing Personal Data outside of College

Disclosing personal data outside of the College: Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act (GDPR). However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way.

8. Checklist for Data Sharing

a) Verify the identity of the caller in response to telephone requests.
b) Make sure they are allowed to share it – that they have the necessary consent.
c) Make sure that the sharing is covered in the Privacy Notice.
d) Ensure adequate security. What is adequate will depend on the nature of the data.

For example:

If the College is sending a child protection report to social services on a memory stick then the memory stick must be encrypted;
Paper information should be sent by courier or recorded delivery, first or second Class post **is not considered secure** enough

9. Sharing other Media

The College should be careful when using photographs, videos or other media as this is covered by the Act as well. Specific guidance on this is provided in the E-Safety and E-Security Policy and the Photography and Videos Policy. All Policies can be found on the College's Website.

Information security and protecting personal data: Information security is the most important aspect of data protection compliance and most of the fines under the Act for non-compliance relate to security breaches.

10. Review Date

These protocols will be reviewed every year by the Head Teacher

Issue Date: 01/11/2020

The next review date for this document is October 2021.